



Программа учебной дисциплины «Безопасность банковской деятельности» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 38.02.07 Банковское дело, утвержденного приказом Министерства образования и науки Российской Федерации от 5 февраля 2018 г. № 67.

Организация-разработчик: АНПОО «Многопрофильная Академия непрерывного образования».

Разработчик: Плотникова И.А., преподаватель.

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>стр. 4</b>
<b>2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>7</b>
<b>3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>11</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>13</b>
<b>5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ</b>	<b>16</b>

# **1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

## **Безопасность банковской деятельности**

### **1.1. Область применения программы**

Программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 38.02.07 Банковское дело.

### **1.2. Место дисциплины в структуре основной профессиональной образовательной программы:**

Дисциплина «Безопасность банковской деятельности» является общепрофессиональной, формирует представления студентов об управлении безопасностью в кредитно-финансовых организациях.

### **1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

В результате освоения дисциплины обучающийся должен уметь:

- выявлять потенциальные угрозы безопасности банка;
- планировать мероприятия по предупреждению угроз безопасности;
- организовывать мероприятия по защите информации.

В результате освоения дисциплины обучающийся должен знать:

- понятие безопасности банковской деятельности, ее основные компоненты;
- классификацию угроз безопасности банка;
- стратегии управления безопасностью;
- подходы к организации службы безопасности банка;
- основные функции руководителя и подразделений службы безопасности;
- понятие конфиденциальной информации и основные мероприятия по обеспечению информационной безопасности;
- мероприятия по защите персонала банка от возможных угроз;
- мероприятия по защите имущества банка от возможных угроз.

## **ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

3.1. В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции.

3.2. Выпускник, освоивший образовательную программу, должен обладать следующими общими компетенциями (далее - ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

3.4. Выпускник, освоивший образовательную программу, должен обладать следующими профессиональными компетенциями (далее - ПК), соответствующими основным видам деятельности:

3.4.1. Ведение расчетных операций:

ПК 1.1. Осуществлять расчетно-кассовое обслуживание клиентов;

ПК 1.2. Осуществлять безналичные платежи с использованием различных форм расчетов в национальной и иностранной валютах;

ПК 1.3. Осуществлять расчетное обслуживание счетов бюджетов различных уровней;

ПК 1.4. Осуществлять межбанковские расчеты;

ПК 1.5. Осуществлять международные расчеты по экспортно-импортным операциям;

ПК 1.6. Обслуживать расчетные операции с использованием различных видов платежных карт.

3.4.2. Осуществление кредитных операций:

ПК 2.1. Оценивать кредитоспособность клиентов;

ПК 2.2. Осуществлять и оформлять выдачу кредитов;

ПК 2.3. Осуществлять сопровождение выданных кредитов;

ПК 2.4. Проводить операции на рынке межбанковских кредитов;

ПК 2.5. Формировать и регулировать резервы на возможные потери по кредитам.

### **1.4. Количество часов на освоение программы дисциплины:**

максимальной учебной нагрузки обучающегося 80 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 8 часов;

самостоятельной работы обучающегося 70 часов

промежуточная аттестация 2 часа.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем учебной дисциплины и виды учебной работы

<b>Вид учебной работы</b>	<b><i>Объем часов</i></b>
<b>Максимальная учебная нагрузка (всего)</b>	80
<b>Обязательная аудиторная учебная нагрузка (всего)</b>	8
в том числе:	
лекции	4
практические занятия	4
<b>Самостоятельная работа обучающегося (всего)</b>	70
<b>Дифференцированный зачёт</b>	2

## 2.2. Тематический план и содержание учебной дисциплины «Безопасность банковской деятельности»

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
<b>Тема 1. Введение. Безопасность банка, ее компоненты</b>		<b>1/6</b>	
	<b>Лекция 1.</b> Предмет и цель курса. Актуальность его изучения. Основные задачи курса. Понятие безопасности банка. Классификация угроз: по целевой направленности; по признаку источника угрозы; по экономическому характеру; по вероятности реализации. Основные компоненты безопасности: информационная безопасность, имущественная безопасность, безопасность персонала. Схема безопасности банка. Особенности управления безопасностью, в том числе российские.	1	1
	<b>Самостоятельная работа</b> обучающихся Изучение теоретического материала [1] Выявить потенциальные угрозы безопасности банка.	6	1,2
<b>Тема 2. Система управления безопасностью банка</b>		<b>3/10</b>	
	<b>Лекция 2.</b> Схема управления безопасностью банка. Операционные подсистемы безопасности: информация, имущество, персонал. Блок обеспечения: информационное, нормативно-методическое, технологическое, инструментальное, трудовое, финансовое. Требования к системе управления безопасностью банка. Оценка эффективности управления.	1	2
	<b>Практическое занятие 1.</b> Технические и электронные средства защиты.	2	2,3
	<b>Самостоятельная работа</b> обучающихся Изучение теоретического материала [1] Написание рефератов. Примерная тематика: 1. Системы оповещения о попытках вторжения. 2. Системы опознавания нарушителей. 3. Механическая защита объекта. 4. Поиск техники подслушивания. Технические средства поиска радиозакладок. 5. Технические средства защиты помещений от подслушивания. 6. Защита технических средств обработки информации. 7. Защита коммуникаций (телефонной и сотовой связи, Bluetooth). Изучите расчетно-кассовое обслуживание клиентов. Виды операций по расчетно-кассовому обслуживанию клиентов. Безналичные платежи с использованием различных форм расчетов в национальной и иностранной валютах. Осуществление расчетного обслуживания счетов бюджетов различных уровней. Межбанковские расчеты. Международные расчеты по экспортно-импортным операциям. Расчетные операции с использованием различных видов платежных карт.	10	1,2
<b>Тема 3. Стратегии управления</b>		<b>10</b>	

безопасностью	<p><b>Самостоятельная работа.</b> Стратегии управления безопасностью: опережающего противодействия, пассивной защиты, адекватного ответа. Положительные и отрицательные стороны стратегий. Факторы, определяющие выбор стратегии. Последовательность реализации выбранной стратегии. Организация мероприятий по защите информации.</p> <p>Задания:</p> <ol style="list-style-type: none"> <li>1. Построение схемы комплекса угроз кредитной организации.</li> <li>2. Оценка надёжности и эффективности функционирования системы безопасности банка.</li> <li>3. Исследование поддельных денежных знаков, ценных бумаг и других документов.</li> <li>4. Право конфиденциальности и система исключительных прав.</li> </ol> <p>Изучите процесс оценки кредитоспособности клиентов. Составьте алгоритм. (Критерии кредитоспособности клиента. Финансовые коэффициенты оценки кредитоспособности клиентов коммерческого банка. Анализ денежного потока как способ оценки кредитоспособности. Оценка кредитоспособности предприятий малого бизнеса. Оценка кредитоспособности физического лица. Оценка кредитоспособности физического лица на основе финансовых показателей его платежеспособности).</p> <p>Изучите процесс оформления выдачи кредитов. Выделите Этапы кредитования физических лиц. Представьте в виде схемы. Осуществление сопровождения выданных кредитов. Проведение операции на рынке межбанковских кредитов. Формирование и регулирование резервов на возможные потери по кредитам.</p>	10	1
<b>Тема 4. Служба безопасности банка, ее функции</b>		4/10	
	<b>Лекция 3.</b> Служба безопасности в структуре банка. Подходы к организации службы безопасности: полный отказ от внешних услуг, максимальное пользование услугами, компромиссный подход. Особенности подходов и организационные структуры. Нормативно-правовая база и планирование деятельности службы. Ресурсное обеспечение. Функции руководителя и основных подразделений службы безопасности. Взаимодействие службы безопасности с другими подразделениями банка.	2	2
	<b>Практическое занятие 2.</b> Системы контроля доступа	2	2,3
	<p><b>Самостоятельная работа</b> обучающихся</p> <p>Изучение теоретического материала [1]</p> <p>Составить план мероприятий по предупреждению угроз безопасности.</p> <p>Написание рефератов. Примерная тематика:</p> <ol style="list-style-type: none"> <li>1. Механические системы. Удостоверения и жетоны. Компьютеризированные системы с применением видео- и фотоизображений.</li> <li>2. Электронные средства контроля доступа (Кнопочные клавиатурные системы контроля доступа. Системы контроля доступа по карточкам. Электронные ключи).</li> <li>3. Биометрические системы контроля доступа. Системы распознавания по отпечаткам пальцев.</li> <li>4. Биометрические системы распознавания по форме кисти руки, по радужной оболочке глаза.</li> <li>5. Биометрические системы распознавания рисунку сетчатки глаза, по голосу.</li> <li>6. Биометрические системы распознавания по геометрии лица, по подписи и клавиатурному почерку. Перспективные биометрические технологии распознавания.</li> </ol>	10	2,3
<b>Тема 5. Информационная</b>		8	



безопасность банка	<p><b>Самостоятельная работа.</b> Понятие конфиденциальной информации. Коммерческая и банковская тайна. Классификация конфиденциальной информации. Нормативные ограничения. Субъекты угроз информационной безопасности. Формы угроз.</p> <p>Изучение теоретического материала [1]</p> <p>Написание рефератов. Примерная тематика:</p> <ol style="list-style-type: none"> <li>1. Виды компьютерного пиратства.</li> <li>2. Безопасность при работе в Интернете.</li> <li>3. Правовые вопросы организации защиты информации.</li> </ol>	8	2
Тема 6. Обеспечение информационной безопасности банка	<p><b>Самостоятельная работа.</b></p> <p>Этапы обеспечения информационной безопасности. Гриф секретности. Каналы утечки информации. Методы защиты информации: программно-математические, технические, организационные. Подсистема информационной безопасности.</p> <p>Утечка различных видов информации.</p> <p>Компьютерная безопасность.</p> <p>Безопасность в компьютерных сетях.</p> <p>Написание рефератов. Примерная тематика:</p> <ol style="list-style-type: none"> <li>1. Криптография.</li> <li>2. Спам и средства борьбы с ним.</li> <li>3. Классификация вредоносных программ.</li> <li>4. Защита от вредоносных программ.</li> <li>5. Парольная защита и методы ее взлома.</li> <li>6. Безопасность электронной почты. Мониторинг электронной почты.</li> <li>7. Профилактика хищения информации сотрудниками организации.</li> <li>8. Пресечение киберслежки (неделового использования Интернета на рабочем месте).</li> </ol>	10	
Тема 7. Безопасность персонала банка	<p><b>Самостоятельная работа.</b> Актуальность защиты персонала. Потенциальные угрозы персоналу. Категории сотрудников банка. Защита от переманивания. Защита от вербовки. Защита от шантажа и угроз в адрес сотрудников. Защита от покушений. Обучение персонала правилам обеспечения безопасности. Контроль персонала.</p>	8	
Тема 8. Имущественная безопасность банка	<p><b>Самостоятельная работа.</b> Имущество банка как объект защиты. Классификация угроз имущественной безопасности банка. Субъекты угроз. Защита от угроз с использованием компьютерных сетей. Защита от угроз при использовании банковских карт. Защита банка от мошенничества при получении кредита. Защита от хищений высоколиквидных активов. Защита от ограблений.</p>	8	
	<b>Дифференцированный зачёт</b>	2	
	<b>Всего:</b>	<b>80</b>	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

#### 3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия кабинета по профилю дисциплины.

##### Оборудование учебного кабинета:

- мебель по количеству студентов,
- доска,
- наглядные пособия, дидактические средства.

##### Технические средства обучения:

- персональные компьютеры,
- мультимедиа-проектор,
- программное обеспечение (Linux Mint, Apache OpenOffice, Kaspersky Anti-Virus (Пробная версия), Консультант Плюс, браузер).

#### 3.2. Информационное обеспечение обучения

##### **Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

Основные источники:

1. Гамза В.А., Ткачук И.Б., Жилкин И.М. Основы банковского дела: безопасность банковской деятельности 4-е изд., пер. и доп. Учебное пособие для спо. Учебное пособие. Изд. 5, пер. и доп. 2023. 432 с. ISBN 978-5-534-13988-4.

Дополнительные источники:

1. Конституция Российской Федерации. – М.: ЭКСМО, 2011.
2. Гражданский кодекс Российской Федерации, ч. I, ч. II. – М.: ЭКСМО, 2011.
3. Уголовный кодекс Российской Федерации. – М.: ЭКСМО, 2011.
4. Федеральный закон «О банках и банковской деятельности». – М.: Омега-Л, 2011.
5. Федеральный закон «О безопасности». – М.: КноРус, 2011.
6. Закон РФ «О частной детективной и охранной деятельности в РФ». – М.: ЭКСМО, 2011.
7. Закон РФ «Об информации, информатизации и защите информации». – М.: Омега-Л, 2006.
8. Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.1991 № 35 М.: «Юридический вестник», № 1, 1991.
9. БАНКОВСКОЕ ДЕЛО в 2 ч. Часть 2. Учебник для СПО, Жуков Е.Ф. - Отв. ред., Соколов Ю.А. - Отв. ред., 2016, 301 с.
10. Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях. – М.: Московская финансово-промышленная академия, 2008.

- 11.Алешин А.П. Техническое обеспечение безопасности бизнеса. - М.: Дашков и Ко, 2008.
- 12.Гамза В.А., Ткачук И.Б. Безопасность банковской деятельности. - М.: Маркет ДС, 2011.
- 13.Гуфан К.Ю., Иванков М.П. Безопасность и эффективность электронных платежных систем в сети Интернет. - М.: Московские учебники - СиДиПресс, 2007.
- 14.Коноплева И.А., Богданов И.А. Управление безопасностью и безопасность бизнеса. - М.: Инфра-М, 2010.
- 15.Кузнецов И.Н. Бизнес-безопасность. - М.: Дашков и Ко, 2010.
- 16.Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. - М.: Академия, 2011.
- 17.Пичугин В. Безопасность бизнеса. Защита от уголовного преследования. - М.: Альпина Пабlishерз, 2009.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Контроль и оценка** результатов освоения дисциплины осуществляется преподавателем в процессе проведения устных опросов, практических занятий, выполнения обучающимися индивидуальных и групповых заданий, контрольной работы, а также в ходе дифференцированного зачета.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
1	2
В результате освоения дисциплины обучающийся должен уметь:	
<ul style="list-style-type: none"> <li>• выявлять потенциальные угрозы безопасности банка;</li> </ul>	<b>Практическое занятие 1.</b> Технические и электронные средства защиты. <b>Практическое занятие 2.</b> Системы контроля доступа <b>Тема 5.</b> Правовые основы защиты информации. Утечка различных видов информации. Безопасность в компьютерных сетях. <b>Тема 6.</b> Компьютерная безопасность.
<ul style="list-style-type: none"> <li>• планировать мероприятия по предупреждению угроз безопасности;</li> </ul>	
<ul style="list-style-type: none"> <li>• организовывать мероприятия по защите информации.</li> </ul>	
В результате освоения дисциплины обучающийся должен знать:	
<ul style="list-style-type: none"> <li>• понятие безопасности банковской деятельности, ее основные компоненты;</li> </ul>	Опрос, деловые ситуации, метод примеров, проведение межпредметных связей с дисциплинами «Менеджмент», «Информатика», «Правовое обеспечение профессиональной деятельности».
<ul style="list-style-type: none"> <li>• классификацию угроз безопасности банка;</li> </ul>	
<ul style="list-style-type: none"> <li>• стратегии управления безопасностью;</li> </ul>	
<ul style="list-style-type: none"> <li>• подходы к организации службы безопасности банка;</li> </ul>	
<ul style="list-style-type: none"> <li>• основные функции руководителя и подразделений службы безопасности;</li> </ul>	
<ul style="list-style-type: none"> <li>• понятие конфиденциальной информации и основные мероприятия по обеспечению информационной безопасности;</li> </ul>	
<ul style="list-style-type: none"> <li>• мероприятия по защите персонала банка от возможных угроз;</li> </ul>	
<ul style="list-style-type: none"> <li>• мероприятия по защите имущества банка от возможных угроз.</li> </ul>	

## **Вопросы к зачету по дисциплине «Безопасность банковской деятельности»**

1. Предмет и цель курса «Безопасность банковской деятельности». Актуальность его изучения. Основные задачи курса.
2. Понятие безопасности банка. Классификация угроз: по целевой направленности; по признаку источника угрозы; по экономическому характеру; по вероятности реализации.
3. Особенности управления безопасностью, в том числе российские.
4. Схема управления безопасностью банка. Блок обеспечения.
5. Требования к системе управления безопасностью банка. Оценка эффективности управления.
6. Стратегии управления безопасностью.
7. Служба безопасности в структуре банка. Подходы к организации службы безопасности.
8. Функции руководителя и основных подразделений службы безопасности.
9. Понятие конфиденциальной информации. Коммерческая и банковская тайна. Классификация конфиденциальной информации.
10. Субъекты угроз информационной безопасности. Формы угроз.
11. Этапы обеспечения информационной безопасности. Гриф секретности. Каналы утечки информации.
12. Методы защиты информации. Подсистема информационной безопасности.
13. Актуальность защиты персонала. Потенциальные угрозы персоналу. Категории сотрудников банка.
14. Защита от переманивания. Защита от вербовки. Защита от шантажа и угроз в адрес сотрудников. Защита от покушений.
15. Обучение персонала правилам обеспечения безопасности. Контроль персонала.
16. Имущество банка как объект защиты. Классификация угроз имущественной безопасности банка. Субъекты угроз.
17. Защита от угроз с использованием компьютерных сетей. Защита от угроз при использовании банковских карт.
18. Защита банка от мошенничества при получении кредита. Защита от хищений высоколиквидных активов. Защита от ограблений.
19. Потенциальные угрозы безопасности банка.
20. Расчетно-кассовое обслуживание клиентов. Виды операций по расчетно-кассовому обслуживанию клиентов.
21. Безналичные платежи с использованием различных форм расчетов в национальной и иностранной валютах.
22. Осуществление расчетного обслуживания счетов бюджетов различных уровней.
23. Межбанковские расчеты.
24. Международные расчеты по экспортно-импортным операциям.

25. Расчетные операции с использованием различных видов платежных карт.
26. Организация мероприятий по защите информации.
27. Угрозы кредитной организации.
28. Оценка надёжности и эффективности функционирования системы безопасности банка.
29. Исследование поддельных денежных знаков, ценных бумаг и других документов.
30. Право конфиденциальности и система исключительных прав.
31. Оценка кредитоспособности клиентов.
32. Оформление выдачи кредитов.
33. Осуществление сопровождения выданных кредитов.
34. Операции на рынке межбанковских кредитов.
35. Формирование и регулирование резервов на возможные потери по кредитам.
36. Мероприятия по предупреждению угроз безопасности.

## 5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата изменения; № страницы с изменением	
<b>БЫЛО</b>	<b>СТАЛО</b>
Основание:	
Подпись лица внесшего изменения	