

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 20.05.2024 15:08:41
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a198149ad36

ПРИЛОЖЕНИЕ 2

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Стерлитамакский филиал

Колледж

Фонд оценочных средств

дисциплина **ОП.17 Безопасность банковской деятельности**

Общепрофессиональный цикл, вариативная часть

цикл дисциплины и его часть (обязательная, вариативная)

38.02.07

код

специальность

Банковское дело

наименование специальности

квалификация

Специалист банковского дела

Разработчик (составитель)

Преподаватель 1 категории

Касьянова В.О.

ученая степень, ученое звание,
категория, Ф.И.О.

Стерлитамак 2024

I Паспорт фондов оценочных средств

1. Область применения

Фонд оценочных средств (ФОС) предназначен для проверки результатов освоения дисциплины ОП 17. «Безопасность банковской деятельности», входящей в состав программы подготовки специалистов среднего звена по специальности 38.02.07 Банковское дело. Работа обучающихся во взаимодействии с преподавателем 52, на самостоятельную работу 20.

2. Объекты оценивания – результаты освоения дисциплины

ФОС позволяет оценить следующие результаты освоения дисциплины:

Уметь:

применять в профессиональной деятельности приемы и методы эффективного делового общения

принимать эффективные решения, используя систему методов управления

составлять системное описание банковских угроз для конкретной кредитной организации

принимать эффективные решения, используя систему методов управления

развитие черт личности, необходимых для безопасного поведения в чрезвычайных ситуациях; бдительности по предотвращению актов терроризма

Знать:

особенности организации управления в банковских учреждениях

необходимость регулирования общественных отношений, сущность социальных норм, механизмы правового регулирования

потенциальные опасности природного, техногенного и социального происхождения

Профессиональные компетенции (ОК)

Вышеперечисленные умения и знания направлены на формирование у обучающихся следующих **общих компетенций**:

ОП.04 Эффективно взаимодействовать и работать в коллективе и команде

ОП.06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных ценностей, применять стандарты антикоррупционного поведения

ОП.07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменениях климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

3 Формы контроля и оценки результатов освоения дисциплины

Контроль и оценка результатов освоения – это выявление, измерение и оценивание результатов освоения дисциплины.

В соответствии с учебным планом специальности 38.02.07 Банковское дело.

Текущий контроль успеваемости представляет собой проверку усвоения учебного материала, регулярно осуществляемую на протяжении курса обучения.

Текущий контроль результатов освоения дисциплины в соответствии с рабочей программой и календарно-тематическим планом происходит при использовании следующих обязательных форм контроля:

- проверка выполнения самостоятельной работы студентов,
- проверка выполнения контрольных работ,

Во время проведения учебных занятий дополнительно используются следующие

формы текущего контроля – устный опрос, решение задач, тестирование по темам отдельных занятий.

Проверка выполнения самостоятельной работы. Самостоятельная работа направлена на самостоятельное освоение и закрепление результатов обучения.

Самостоятельная подготовка обучающихся по дисциплине предполагает следующие виды и формы работы:

- Систематическая проработка конспектов занятий, учебной и специальной технической литературы.
- Самостоятельное изучение материала и конспектирование лекций по учебной и специальной технической литературе.
- Написание и защита доклада; подготовка к сообщению или беседе на занятии по заданной преподавателем теме.
- Выполнение расчетных заданий.
- Работа со справочной литературой и нормативными материалами.
- Составление тестовых заданий по темам УД/МДК.

Список практических работ:

Практическая работа № 1

Задание: Проанализировать причины совершения и дать характеристику наиболее характерным преступлениям в банковской сфере России

Алгоритм решения задания:

- 1 Составить кластер «Классификация преступлений в банковской сфере России»
- 2 Составить таблицу «Насильственные преступления в отношении персонала и имущества банков»
- 3 Составить таблицу «Финансовые преступления в сфере банковской деятельности»
- 4 По материалам периодических изданий и сайтов Интернет подготовить доклад о совершенном преступлении в банковской сфере

Практическая работа № 2

Задание: Провести анализ защищенности конфиденциальной банковской информации

Алгоритм решения задания

- 1 Составить таблицу «Меры по защите конфиденциальной информации, предпринимаемые в банке»
- 2 По материалам периодических изданий и сайтов Интернет подготовить доклад о последствиях утечки конфиденциальной банковской информации

Практическая работа № 3

Задание: Провести анализ проблем безопасности электронных платежей и банковских платежных карт

Алгоритм решения задания

- 1 Составить таблицу Способы мошенничества с пластиковыми картами
- 2 По материалам периодических изданий и сайтов Интернет подготовить доклад о проблемах безопасности электронных платежей и банковских платежных карт

Практическая работа № 4

Задание: Провести анализ механизма взаимодействия с органами МВД в обеспечении безопасности банка

Алгоритм решения задания

- 1 С помощью системы КонсультантПлюс изучить как Уголовный Кодекс РФ регулирует отношения по поводу обеспечения безопасности банка путем установления уголовно- правовой охраны от преступлений
- 2 С помощью системы КонсультантПлюс изучить Соглашение между МВД России и Ассоциацией российских банков о взаимодействии в области обеспечения банковской

безопасности и рассмотреть основные направления такого взаимодействия

Практическая работа № 5

Задание: Провести анализ действия службы безопасности и сотрудников банка в кризисных ситуациях

Алгоритм решения задания

- 1 Составить перечень возможных кризисных ситуаций в банковской деятельности
- 2 По материалам периодических изданий и сайтов Интернет подготовить доклад о действиях службы безопасности и сотрудников банка в кризисных ситуациях

Практическая работа № 6

Задание: Изучить инженерно-технические средства охраны, средства самозащиты, специальный транспорт

Алгоритм решения задания

- 1 составить кластер «Классификация технических средств защиты банковской тайны»
- 2 По материалам периодических изданий и сайтов Интернет подготовить доклад о современных технических средствах защиты банковской тайны

Практическая работа № 7

Задание №1. Сотрудник отдела безопасности банка принимает решение о возможности выдачи кредита физическому лицу. Частный клиент предоставил справку с места работы о среднемесячном доходе в размере 178 000 рублей. Как проверить работнику отдела безопасности финансово-кредитной организации достоверность информации, содержащейся в справке клиента?

Задание №2. Мошенник желает осуществить операцию покупки, расплатившись в торгово-сервисном предприятии картой, подделанной путём перекодирования информации, содержащейся на магнитном носителе (внешние реквизиты и данные магнитного носителя не совпадают). Каким образом кассовой сотрудник торгово-сервисной точки может узнать, что карта поддельная?

Практическая работа № 8

Задание №1. Клиент проводит операцию по оплате налоговых платежей, которую он совершает наличными деньгами на общую сумму 56 000 рублей. При введении сотрудником кредитной организации идентификационных данных клиента в программу банка по проведению платежей, машина высветила информацию, что данный клиент находится в списках экстремистов и террористов. Какие должны последовать за этим действия операционно-кассового сотрудника банка?

Задание №2. С каким кодом(ами) обязательного контроля подлежит отправки в Федеральную службу по финансовому мониторингу следующая операция: Физическое лицо открывает обезличенный металлический счёт в золоте, при этом в кассу банка он вносит не слитки, а 780 000 рублей.

Практическая работа № 9

Задание №1. У сотрудника банка по работе с клиентами возникли сомнения относительно подлинности платёжного поручения на списание денежных средств со счёта юридического лица, предоставленного в банк. Какие дальнейшие действия должны последовать со стороны операционно-кассового сотрудника?

Практическая работа № 10

Проблема Мошенники изобрели массу способов изъятия денег с чужой банковской карты.

Как в современных условиях максимально обезопасить свои средства?

Задание Составьте десять правил пластиковой безопасности.

Практическая работа № 11

1. Бюро кредитных историй и их роль в обеспечении безопасности банка.
2. Понятие финансовой безопасности коммерческого банка и ее составляющие.
3. Организация противодействия (легализации) отмыванию доходов, полученных преступным путем и финансированию терроризма.
4. Вольфсбергские принципы финансовой безопасности банка.

Проверка выполнения самостоятельной работы. Самостоятельная работа направлена на самостоятельное освоение и закрепление обучающимися практических умений и знаний, овладение профессиональными компетенциями.

Самостоятельная подготовка обучающихся по дисциплине предполагает следующие виды и формы работы:

- *Систематическая проработка конспектов занятий, учебной и специальной литературы.*
- *Самостоятельное изучение материала и конспектирование лекций по учебной и специальной литературе.*

Проверка выполнения контрольных работ. Контрольная работа проводится с целью контроля усвоенных умений и знаний и последующего анализа типичных ошибок и затруднений обучающихся в конце изучения темы или раздела. Согласно календарно-тематическому плану дисциплины предусмотрено проведение следующих контрольных работ:

Тестовые задания

1. Безопасность – это:
 - а) Специфическая совокупность внешних и внутренних условий деятельности, позволяющих субъекту контролировать процесс собственного существования и достигать намеченных целей указанной деятельности;
 - б) Источник потенциального ущерба имуществу или инфраструктуре банка, причинение которого может воспрепятствовать достижению банка установленных целей;
 - в) Мера допустимо опасных условий деятельности банка, неблагоприятные последствия которых реализуются в связи с ошибочными действиями или бездействием персонала банка.
2. По экономическому характеру угрозы делятся на:
 - а) Потенциальные, реализуемые угрозы;
 - б) Угрозы со стороны конкурентов, со стороны персонала банка;
 - в) Угрозы имущественного и неимущественного характера.
3. К важной для банка информации относится:
 - а) Незаменимая информация, утечка или разрушение которой ставят под угрозу само функционирование кредитной организации;
 - б) Информация, утечка или разрушение которой наносит материальный ущерб кредитной организации, однако она может эффективно функционировать и после этого;
 - в) Информация, процесс ликвидации последствий утечки или разрушения которой сложен или связан с большими затратами.
4. Для банков ориентированных на обслуживание высокорентабельных предприятий (отраслей), наиболее целесообразным вариантом стратегии обеспечения собственной безопасности является:
 - а) Стратегия «упреждающего противодействия»;
 - б) Стратегия «адекватного противодействия»;
 - в) Стратегия «пассивной защиты».
5. Деятельность отдела собственной безопасности в составе службы безопасности банка направлен на контроль:
 - а) высших руководителей банка;
 - б) сотрудников самой службы безопасности;
 - в) эффективности управления безопасностью банка в целом.
6. В обучении новых сотрудников банка правилам обеспечения его безопасности должны принимать участие:

- а) Сотрудники службы безопасности;
 - б) Сотрудники службы персонала;
 - в) Руководители их структурных подразделений;
 - г) Все перечисленные выше специалисты банка.
7. При нападении на банк персоналу необходимо:
- а) Не выполнять все требования нападавших, так как они влекут за собой впоследствии банкротство банка;
 - б) Выполнять абсолютно все требования нападавших, даже если они влекут за собой впоследствии банкротство банка;
 - в) Действовать на своё усмотрение.
8. Задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях:
- а) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях;
 - б) Защита информации от несанкционированного доступа;
 - в) Обеспечение достоверности, идентификации и сохранности информации при ее передаче по каналам связи;
9. Коммерческая тайна – это:
- а) Информация по счетам или вкладам своих клиентов и корреспондентов;
 - б) Любая информация, обеспечивающая достижение преимуществ над конкурентами и извлечение прибыли;
 - в) Информация об объемах и структуре предоставленных и полученных кредитов и депозитов.
10. Механизм электронной цифровой подписи реализует функции:
- а) Шифрование, сертификация;
 - б) Аутентификация, шифрование;
 - в) Сертификация, аутентификация.
11. Промышленный шпионаж – это:
- а) получение обманным путем конфиденциальной информации, используемой в различных противоправных целях;
 - б) уголовно наказуемое и иное противоправное деяние, посягающее на имущественные и приравненные к ним права и интересы банка либо на порядок его функционирования;
 - в) присвоение кредитов по фиктивным банковским гарантиям подставными фирмами.
12. Внутренняя безопасность включает:
- а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы;
 - б) Защиту от несанкционированного доступа к информации;
 - в) Защиту от случайных внешних воздействий;
13. Криптография – это:
- а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
 - б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации;
 - в) Наука о методах обеспечения конфиденциальности и аутентичности информации.
14. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:
- а) Стратегия адекватного ответа;

- б) Стратегия пассивной защиты;
 - в) Упреждающего противодействия.
15. Финансовые махинации относятся к ... преступлениям в банковской сфере:
- б) насильственным;
 - в) «беловоротничковым»;
 - г) Экономическим.

II вариант

1. Внешняя безопасность включает:
- а) Регламентацию доступа пользователей и обслуживающего персонала к информации системы;
 - б) Защиту от несанкционированного доступа к информации;
 - в) Регламентацию доступа пользователей и обслуживающего персонала к ресурсам системы.
2. По признаку целевой направленности угрозы делятся на:
- а) Угроза разглашения конфиденциальной информации, угроза имуществу банка;
 - б) Угрозы со стороны конкурентов и со стороны криминальных структур;
 - в) Угрозы имущественного характера и неимущественного характера.
3. Что относится к организационно-управленческой информации, которая входит в состав коммерческой тайны:
- а) Источники и объёмы финансирования и кредитования;
 - б) Базы данных по клиентам;
 - в) Базы данных о ведущих специалистов банка.
4. Главным элементом криптосистемы считаются:
- а) Алгоритмы шифрования;
 - б) Методы распространения ключей к этим шифрам;
 - в) Обе группы указанных элементов в равной степени.
5. К насильственным преступлениям в банковской сфере относятся:
- а) Грабежи;
 - б) Финансовые хищения;
 - в) Махинации
6. К «беловоротничковым» преступлениям в банковской сфере относятся:
- а) Грабежи;
 - б) Финансовые хищения;
 - в) Налёты на обменные пункты.
7. Налёты на обменные пункты относятся к ... преступлениям в банковской сфере:
- а) насильственным;
 - б) «беловоротничковым»;
 - в) Экономическим.
8. Аутентификация – это:
- а) Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
 - б) Реквизит электронного документа, предназначенный для защиты данного документа от модификации;
 - в) Наука о методах обеспечения конфиденциальности и аутентичности информации.
9. К полезной банковской информации относится:
- а) Незаменимая информация, утечка или разрушение которой ставят под угрозу само функционирование кредитной организации;
 - б) Информация, утечка или разрушение которой наносит материальный ущерб кредитной организации, однако она может эффективно функционировать и после этого;

- в) Информация, процесс ликвидации последствий утечки или разрушения которой сложен или связан с большими затратами.
- 10. Данные составляющие банковскую тайну:
 - а) Объёмы инвестиций, планы маркетинга;
 - б) Базы данных об акционерах и специалистах;
 - в) Информация банковского вклада, операций по счёту и сведений о клиенте.
- 11. Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз:
 - а) Стратегия адекватного ответа;
 - б) Стратегия пассивной защиты;
 - в) Упреждающего противодействия.
- 12. Задача проведения анализа уязвимости информационной банковской системы:
 - а) Рассмотрение всех возможных угроз и оценка размеров возможного ущерба;
 - б) Определение всех возможных слабых мест информационной банковской системы;
 - в) Регламентация деятельности кредитной организации.
- 13. При реализации, какой концепции допускаются банковский шпионаж, не всегда легитимные методы контроля:
 - а) Стратегия адекватного ответа;
 - б) Стратегия пассивной защиты;
 - в) Упреждающего противодействия.
- 14. Задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях:
 - а) Обеспечение сохранности информации, как в памяти ЭВМ, так и на отдельных носителях;
 - б) Обеспечение достоверности, идентификации и сохранности информации при ее передаче по каналам связи;
 - в) Защита информации от несанкционированного доступа;
- 15. По вероятности практической реализации угрозы делятся на:
 - а) Имущественного и неимущественного характера;
 - б) Угрозы со стороны нелояльных сотрудников и конкурентов;
 - в) Потенциальные и реализованные угрозы.

I вариант

1. Что включает в себя безопасность банковской деятельности?
 - 1) привлечение потенциальных опасностей
 - 2) отсутствие опасностей
 - 3) поступление информации от потребителей
 - 4) нет верного ответа
2. Угрозы финансовых ресурсов проявляются в виде:
 - 1) не возврата кредитных сумм, хищения финансовых средств из банкомата и инкассаторских машин
 - 2) нападения, вторжения, захвата
 - 3) вымогательства значительных сумм денежных средств, льгот перед лицом террористической угрозы
 - 4) обстрела из огнестрельного оружия
3. По характеру воздействия угрозы классифицируют на:
 - 1) вероятные, весьма вероятные, маловероятные
 - 2) стихийные, преднамеренные
 - 3) предельные, значительные, незначительные

- 4) активные, пассивные
4. Субъектами правоотношений при решении проблемы безопасности являются:
- 1) государство
 - 2) юридические и физические лица
 - 3) службы безопасности банков и частные охранные структуры
 - 4) верны все ответы
5. Что НЕ относится к экономическому преступлению?
- 1) хищение финансовых и материальных средств
 - 2) изготовление поддельных денег
 - 3) обман потребителей
 - 4) рекламирование своей продукции
6. Что НЕ относится к основной деятельности по обеспечению безопасности банка?
- 1) безопасность персонала
 - 2) безопасность информационных ресурсов
 - 3) сохранность и физическая защита материальных и финансовых средств и объектов
 - 4) подбор и расстановка кадров
7. Что НЕ относится к преступлению в сфере экономики?
- 1) преступление против собственности
 - 2) преступление против чести, свободы и достоинства
 - 3) заведомо ложная реклама
 - 4) незаконное предпринимательство
8. Безопасность - это...
- 1) наука, которую надо изучать
 - 2) наука, которую надо развивать
 - 3) искусство, которое надо постигать
 - 4) наука, которую надо изучать и развивать, искусство, которое надо постигать, культура, которую надо воспитывать у предпринимателей
9. К видам негативных воздействий злоумышленников относятся:
- 1) экономическое подавление
 - 2) физическое подавление
 - 3) экономическое, физическое, финансовое, информационное, психическое подавление
 - 4) нет верного ответа
10. Ущерб от угроз бывает:
- 1) материальный и моральный
 - 2) физический
 - 3) психологический
 - 4) интеллектуальный
11. Финансовые средства, материальные ценности и новейшие технологии - это...
- 1) субъекты безопасности
 - 2) объекты безопасности
 - 3) органы безопасности
 - 4) задачи безопасности
12. Безопасность на рынке финансов - это...
- 1) основа бизнеса
 - 2) состояние защищенности
 - 3) обеспечение устойчивости финансирования
 - 4) охрана руководителей
13. Преступные посягательства (угрозы) совершают в целях...
- 1) собственной выгоды

- 2) получения материального и морального удовлетворения
 - 3) нанесения ущерба
 - 4) создания служб безопасности для сокращения безработицы
14. Мошенничество - это...
- 1) форма хищения по средствам насилия или убийства с целью завладения заведомо чужим имуществом
 - 2) одно из преступлений против личности, наносящее вред здоровью личности
 - 3) одно из преступлений против собственности, одна из форм хищения, представляющая собой завладение чужим имуществом путём обмана или злоупотреблением доверием
 - 4) нет верного ответа
15. Способами мошенничества являются:
- 1) злоупотребление доверием, разбой
 - 2) нападение, разбой
 - 3) обман, нападение
 - 4) обман, злоупотребление доверием

II вариант

1. Источниками мошенничества являются:
- 1) форс-мажорные обстоятельства
 - 2) законопослушные граждане
 - 3) хакеры
 - 4) нет верного ответа
2. К внутренним условиям мошенничества можно отнести:
- 1) недоверчивость
 - 2) некомпетентность, безответственность
 - 3) несовершенство личности
 - 4) все ответы верны
3. К каким источникам опасности относят следующие объекты: подкуп персонала, перехват сообщений, съём информации со специальной аппаратуры?
- 1) к персоналу
 - 2) к конкурентам
 - 3) к недобросовестным контрагентам
 - 4) к техногенным катастрофам
4. Что относится к психологическому давлению злоумышленников?
- 1) угрозы и шантаж
 - 2) сокращение производства
 - 3) мошенничество
 - 4) устранение сотрудников и руководства
5. К какому виду преступлений относится данная характеристика: операционные системы, системы управления базами данных, пароли?
- 1) подмена
 - 2) кража
 - 3) перехват информации
 - 4) уничтожение
6. Действия злоумышленников могут быть:
- 1) параллельные
 - 2) вертикальные, горизонтальные
 - 3) международные
 - 4) внешние и внутренние
7. Политика безопасности банка представляет собой:
- 1) непрерывность
 - 2) экономность
 - 3) систему взглядов (мер, решений)

- 4) нет верного ответа
8. К финансовым преступлениям в сфере банковской деятельности относят:
- 1) лжекредитование
 - 2) залог
 - 3) страховку
 - 4) консалтинг
9. К основным приёмам деятельности преступных группировок относят:
- 1) террор
 - 2) саботаж
 - 3) сращивание экономической и уголовной преступности
 - 4) нет верного ответа
10. В классификации источников внутренних угроз банка выделяют:
- 1) финансовые преступления
 - 2) организованную преступность
 - 3) шпионаж
 - 4) нет верного ответа
11. Обеспечение экономической безопасности банка является прерогативой...
- 1) Министерства Внутренних Дел
 - 2) Федеральной службы безопасности
 - 3) Министерства финансов
 - 4) администрации банка
12. Правовое регулирование коммерческой безопасности распространяется на:
- 1) банки
 - 2) торговые точки
 - 3) спецфонды
 - 4) благотворительные организации
13. Обеспечение личной безопасности банковских служащих является задачей:
- 1) прокуратуры
 - 2) милиции
 - 3) самих банковских служащих
 - 4) нет верного ответа
14. К видам безопасности относят:
- 1) залог
 - 2) гарантию
 - 3) страховку
 - 4) геобиофизическую, техническую, общественную безопасность
15. К угрозам банковской безопасности по объекту посягательства относятся:
- 1) политические угрозы
 - 2) криминальные угрозы
 - 3) информационные угрозы
 - 4) нет верного ответа

І вариант

1. Какие реквизиты должны содержать защищенные документы?
- 1) регистрационный номер, товарный знак
 - 2) название фирмы
 - 3) дату создания документа
 - 4) основные реквизиты
2. К числу преступлений в компьютерной сфере относят:
- 1) аппаратные сбои
 - 2) перегрузку
 - 3) перехват информации

- 4) вирусы
3. К защите банковской информации в автоматизированной системе обработки относят:
- 1) моральную, политическую, производственную ответственность граждан
 - 2) технологические приобретения, установку и использование защит-ных средств от различного рода воздействий технических средств обработки информации
 - 3) персонал
 - 4) новейшие технологии
4. К видам угроз утечки информации при автоматизированной обработке относят:
- 1) банковскую тайну
 - 2) профессиональную тайну
 - 3) отказы и сбои в работе аппаратуры
 - 4) нет верного ответа
5. К основным техническим каналам утечки банковской информации относят:
- 1) разговорный
 - 2) телефонный
 - 3) электромагнитный
 - 4) нет верного ответа
6. Обеспечение информационной безопасности банковских систем достигается путём:
- 1) факса
 - 2) электронных платежей
 - 3) телефона
 - 4) ксерокса
7. Какой разновидности пластиковых карт нет?
- 1) интеллектуальных
 - 2) кредитных
 - 3) дебетовых
 - 4) клиринговых
8. Уязвимые места защиты в системах обмена электронными данными (ОЭД):
- 1) пересылка платёжных и других сообщений между банками или между банком и клиентом
 - 2) обработка информации внутри организаций отправителя и получателя
 - 3) доступ клиента к средствам, аккумулированным на счёте
 - 4) все ответы верны
9. Что НЕ относится к угрозам безопасности по принципу воздействия на автоматизированную систему обработки информации банка?
- 1) использование доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.)
 - 2) использование закрытых каналов связи
 - 3) использование открытых каналов связи
 - 4) воздействие на систему разрешений (в т.ч. захват привилегий)
10. Укажите угрозы безопасности автоматизированной системы обработки информации банка по способу воздействия на объект атаки:
- 1) непосредственное воздействие на объект атаки
 - 2) воздействие на систему разрешений (в том числе захват привилегий)
 - 3) опосредованное воздействие (через других пользователей)
 - 4) все ответы верны
11. Какие типы PIN- кодов существуют?
- 1) назначаемые выведенные
 - 2) назначаемые случайные
 - 3) выбираемые пользователем
 - 4) все ответы верны

12. Идентификация клиента с использованием PIN-кодов работает в случаях:

- 1) отсутствия перехвата карточки
- 2) воровства банковских карточек
- 3) невозможности доступа к системе другим пользователем
- 4) все ответы верны

13. Что произойдет при вводе неверного PIN-кода?

- 1) "самоблокировка" карточки
- 2) включение сигнализации
- 3) автоматическое уничтожение карточки
- 4) нет верного ответа

14. Недостаток интеллектуальной карточки:

- 1) низкая стоимость производства карточки
- 2) уменьшенная по сравнению со стандартом толщина карточки и объём информации
- 3) высокий процент за обслуживание
- 4) увеличенная по сравнению со стандартом толщина карточки и высокая стоимость производства карточки

15. Что НЕ относится к защите пластиковой карточки?

- 1) торговое имя продукта
- 2) вокруг панели расположена кайма печатных кодов идентификации банка
- 3) поле fine-line в области идентификации продукции
- 4) трехмерная голограмма голубя

II вариант

1. Задачи автоматического кассового аппарата:

- 1) идентификация и аутентификация клиента
- 2) выдача наличных денег
- 3) оповещение о состоянии счета клиента
- 4) все ответы верны

2. К эмитенту карточки предъявляются требования:

- 1) карточка должна восприниматься вручную
- 2) карточка не должна обладать технологией проверки собственных обменных PIN-кодов
- 3) карточка не должна соответствовать правильности PIN-кодов
- 4) карточка должна восприниматься автоматически и обладать технологией проверки собственных обменных PIN-кодов

3. Виды защиты информации:

- 1) средства физической защиты
- 2) программные средства
- 3) административные меры защиты
- 4) все ответы верны

4. Что относится к угрозам конфиденциальной информации в нарушении конфиденциальности?

- 1) разглашение
- 2) утечка
- 3) НСД (несанкционированный доступ)
- 4) все ответы верны

5. Что относится к угрозам конфиденциальной информации в нарушении доступности?

- 1) изменение информации
- 2) закрытый доступ получения информации
- 3) нарушение связи, запрет получения информации
- 4) нет верного ответа

6. Разглашение конфиденциальной информации проявляется в виде:

- 1) сообщения (передачи, предоставления)
 - 2) пересылки
 - 3) опубликования
 - 4) все ответы верны
7. К факторам и обстоятельствам, способствующим утечке конфиденциальной информации относится:
- 1) недостаточное знание сотрудником правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения
 - 2) использование неаттестованных технических средств обработки конфиденциальной информации
 - 3) слабый контроль за соблюдением правил защиты информации право-выми, организационными и инженерно-техническими мерами
 - 4) все ответы верны
8. Источники угроз несанкционированного доступа:
- 1) конкуренты
 - 2) преступники
 - 3) административные органы
 - 4) верны все ответы
9. Утечка конфиденциальной информации - это...
- 1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
 - 2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
 - 3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
 - 4) нет верного ответа
10. Разглашение - это...
- 1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
 - 2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
 - 3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
 - 4) нет верного ответа
11. Несанкционированный доступ - это...
- 1) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
 - 2) умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к ознакомлению с ними лиц, не допущенных к ним
 - 3) преднамеренные противоправные действия злоумышленников с целью получения охраняемых сведений
 - 4) нет верного ответа
12. В какой форме оформляется обязательство о неразглашении конфиденциальной информации при переводе сотрудника на другую работу, связанную с конфиденциальной информацией, а так же при увольнении сотрудника?
- 1) в письменном
 - 2) в устном
 - 3) по усмотрению службы безопасности
 - 4) нет правильного ответа
13. К угрозам информационных ресурсов относится:

- 1) разглашение конфиденциальной информации
 - 2) подслушивание конфиденциальных переговоров в служебных помещениях
 - 3) подлог платёжных документов и пластиковых карт
 - 4) информационно-психологическое воздействие
14. Правовой основой банковского бизнеса служит:
- 1) страхование
 - 2) залог
 - 3) закон "О банках и банковской деятельности"
 - 4) нет верного ответа
15. Правовая основа защиты конфиденциальной банковской информации базируется на:
- 1) депозитах
 - 2) кредитах
 - 3) банковской тайне (профессиональной тайне)
 - 4) нет верного ответа
-
1. По характеру защитных мероприятий инженерно-технические средства защиты классифицируются:
- 1) организационные, системные, банковские
 - 2) организационные, технические, организационно-технические
 - 3) технические, банковские, внебанковские
 - 4) организационные, инженерные
2. Какие виды защиты информации используются в линиях связи?
- 1) магнитные преобразования информации
 - 2) незащищенные волоконно-оптические линии связи
 - 3) жучки
 - 4) криптографические преобразования информации и защищенные волоконно-оптические линии связи
3. Инкассаторская автомашина НЕ отвечает требованиям:
- 1) бронированная защита кузова
 - 2) улучшенные ходовые характеристики
 - 3) двери кабины водителя и кузова имеют специальные внутренние запорные устройства
 - 4) звукоизоляция кузова
4. На какие группы подразделяются технические средства защиты?
- 1) средства труда, оборотные средства
 - 2) средства оповещения, средства первой медицинской помощи
 - 3) средства охраны, средства защиты информации
 - 4) нет верного ответа
5. Какие из перечисленных средств относятся к информационной безопасности компьютерных сетей?
- 1) управляющая электроника и программное обеспечение
 - 2) средства учёта и контроля автотранспорта
 - 3) антикражная система
 - 4) биометрические средства защиты информации
6. К инженерно-техническим средствам защиты относятся:
- 1) сейфы и оборудование банковских хранилищ, банкоматы и др.
 - 2) транкинговые системы
 - 3) средства производственной и пожарной информатики
 - 4) информационные системы

7. Какие технологии средства НЕ относятся к системам связи и оповещения?
- 1) транкинговые системы
 - 2) профессиональные, носимые, мобильные и базовые радиостанции
 - 3) учрежденческие АТС, системы конференц-связи
 - 4) аварийно-спасательная техника
8. Какие технологические средства относятся к системам связи и оповещения?
- 1) сейфы и специальные шкафы
 - 2) оборудование банковских хранилищ
 - 3) системы тревожного оповещения
 - 4) пожарная техника
9. Услуги, средства поддержки и обслуживания систем безопасности...
- 1) системы бесперебойного питания и автономные энергоустановки
 - 2) суда, катера и другие плавсредства
 - 3) транкинговые системы
 - 4) специальная одежда, обувь и обмундирование
10. Вход для клиентов оборудуется следующими техническими средствами:
- 1) учрежденческими АТС
 - 2) специальными сетями связи и информационными системами
 - 3) кнопкой тревожной сигнализации, устройствами дистанционного управления, входными и выходными дверями
 - 4) монтажным оборудованием и инструментом
11. Входной тамбур и место дежурства сотрудника охраны должны быть оборудовано следующими техническими средствами:
- 1) телефонным аппаратом прямой связи с центральным пунктом охраны, кнопкой тревожной сигнализации, датчиком открывания дверей
 - 2) аварийно-спасательным инструментом
 - 3) оборудованием для специальных автомобилей, судами, катерами и другими плавсредствами
 - 4) контрольно- измерительной аппаратурой
12. Зона кассиров должна иметь следующие технические средства:
- 1) автомобили для перевозки денежных средств и ценностей
 - 2) кнопку тревожной сигнализации (ручную или ножную) телекамеру, датчики открытия, закрытия дверей
 - 3) оборудование для специальных автомобилей
 - 4) обнаружители наркотических средств, металлодетекторы

13. Защита от перехвата побочных, электромагнитных измерений и наводок самого различного характера обеспечивается...

- 1) экранированием помещений средств канальных коммуникаций, использованием автономных телефонных систем, локальных систем ЭВМ, не имеющих выхода за пределы охраняемой территории и др.
- 2) аварийно-спасательной техникой, оборудованием для специальных автомобилей
- 3) системой вентиляции и кондиционированием воздуха, контрольно-измерительной аппаратурой
- 4) страхованием и детективной деятельностью, физической охраной объектов

14. К антитеррористическому и досмотровому оборудованию относятся:

- 1) стенографические средства защиты и передачи информации
- 2) металлодетекторы, рентгеновское оборудование, системы радиационного мониторинга, обнаружители наркотических веществ
- 3) автоматизированные системы управления интеллектуальным зданием, комплекс систем информации
- 4) автоматизированные средства защиты

15. Кризисная ситуация - это...

- 1) проявление факторов угроз со стороны отдельных лиц или групп
- 2) слабость в средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для проникновения в систему
- 3) проявление факторов угроз со стороны массовых групп
- 4) нет верного ответа

II вариант

1. Что НЕ относится к принципам организации и функционирования системы безопасности?

- 1) непрерывность
- 2) своевременность
- 3) бесконечность
- 4) нет верного ответа

2. Комплексный принцип организации и функционирования системы безопасности подразумевает:

- 1) защиту интересов банка с достаточной степенью настойчивости, широко используемую силу, средства обеспечения безопасности и нестандартные методы защиты
- 2) обеспечение безопасности персонала, материальных, финансовых ресурсов от возможных угроз всеми доступными законными средствами, мерами и мероприятиями
- 3) совершенствование мер и средств защиты на основе собственного опыта, появление новых технических средств с учетом изменения методов и средств разведки и промышленного шпионажа
- 4) привлечение к разработке и внедрению средств защиты специализированных органов

3. Главные цели системы безопасности:

- 1) обеспечение устойчивого функционирования банка и предотвращение угроз

по безопасности

2) защита законных интересов от противоправных посягательств, охраны жизни и здоровья персонала и недопущение хищения финансовых и материально-технических средств

3) обеспечение неустойчивости функционирования банка

4) нет верного ответа

4. На какой правовой нормативный акт необходимо опираться при практическом решении задач обеспечения безопасности банка?

1) на устав банка

2) на приказ руководителя банка

3) на заявление физического лица

4) на положение о государственной системе защиты информации от инженерно-технических работ и от утечки

5. К основным задачам службы безопасности относится:

1) выявление и локализация возможных каналов утечки конфиденциальной информации, обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания

2) информация о порядке работы с иностранными представителями

3) безопасность информационных ресурсов

4) безопасность персонала

6. Кто возглавляет службу безопасности в банке?

1) начальник в должности заместителя руководителя банка по безопасности

2) руководитель банка

3) начальник отдела безопасности

4) нет верного ответа

7. В службу безопасности НЕ входит следующая структурная служба:

1) подразделение обновления системы

2) подразделение режима и охраны

3) подразделение инженерно-технической защиты

4) подразделение информационно-аналитической деятельности

8. Что НЕ относится к действиям частных детективов?

1) защита жизни и здоровья граждан

2) наведение справок

3) внешний осмотр строений, помещений

4) слежка за объектами

9. Для чего предназначена охранная система?

1) для ограничения круга лиц, имеющих доступ к документам, обеспечения оптимального режима пользования теми лицами, кому они доверены

2) для ограничения круга лиц, имеющих доступ к документам

3) для обеспечения оптимального режима к информации

4) для охраны жизни и здоровья членов семей работников банка

10. К основным кризисным ситуациям в работе банков относят:

1) взятие заложников

2) забастовку

3) демонстрацию

4) нет верного ответа

11. При каких условиях органам предварительного следствия предоставляется информация, составляющая банковскую тайну?

1) с согласия руководителя банка

2) с согласия прокурора и клиента банка

3) с согласия клиента банка

4) по возбужденным уголовным делам и с согласия прокурора

12. Кому выдаются справки по счетам и вкладам физических лиц банком?
- 1) клиенту
 - 2) суду
 - 3) органам предварительного следствия по делам, находящимся в их производстве, с согласия прокурора
 - 4) все ответы верны
13. Система безопасности - это...
- 1) организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих, защиту жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз
 - 2) финансовые мероприятия по защите информации с целью минимизации рисков утраты или изменения информации и уменьшения страхового возмещения
 - 3) финансовые мероприятия по защите населения
 - 4) нет верного ответа
14. Основными элементами системы безопасности банка являются:
- 1) ответственный руководитель системы и клиенты банка
 - 2) совет безопасности и клиенты банка
 - 3) ответственный руководитель системы и совет безопасности банка
 - 4) нет верного ответа
15. На основе каких организационно-правовых документов действует система безопасности?
- 1) устава банка
 - 2) положения о системе безопасности
 - 3) руководства по защите конфиденциальной информации
 - 4) верны все ответы

Сводная таблица по применяемым формам и методам текущего контроля и оценки результатов обучения

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Освоенные умения:	
применять в профессиональной деятельности приемы и методы эффективного делового общения принимать эффективные решения, используя систему методов управления	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия
составлять системное описание банковских угроз для конкретной кредитной организации	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия
принимать эффективные решения, используя систему методов управления развитие черт личности, необходимых для безопасного поведения в чрезвычайных ситуациях; бдительности по предотвращению актов терроризма	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия
Усвоенные знания:	
особенности организации управления в банковских учреждениях	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия

необходимость регулирования общественных отношений, сущность социальных норм, механизмы правового регулирования	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия
потенциальные опасности природного, техногенного и социального происхождения	Выполнение практической работы Оценка правильности выполнения самостоятельной работы по темам Устный опрос во время занятия

3.2 Форма промежуточной аттестации

Промежуточная аттестация по дисциплине _ОП 17. «Безопасность банковской деятельности» – зачет оценкой в 6 семестре.

Обучающиеся допускаются к сдаче зачета при выполнении всех видов самостоятельной работы, предусмотренных рабочей программой и календарно-тематическим планом дисциплины.

Перечень вопросов к зачету

1. Понятие и концепция безопасности банка.
2. Классификация угроз банковской деятельности.
3. Управление безопасностью банка.
4. Факторы, влияющие на безопасность банка.
5. Основные составляющие безопасности банковской деятельности.
6. Организационные основы безопасности банковской деятельности.
7. Организация внутреннего контроля банка и службы безопасности коммерческого банка.
8. Техника обеспечения безопасности банка.
9. Объекты защиты в системе безопасности банка.
10. Бюро кредитных историй и их роль в обеспечении безопасности банка.
11. Понятие финансовой безопасности коммерческого банка и ее составляющие.
12. Организация противодействия (легализации) отмыванию доходов, полученных преступным путем и финансированию терроризма.
13. Принципы финансовой безопасности банка

4 Система оценивания комплекта ФОС текущего контроля и промежуточной аттестации

Каждый вид работы оценивается по пяти бальной шкале.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «5» (отлично) предполагает грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Критерии оценивания ответа по устному опросу.

«5» (отлично) – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения; за грамотное и логичное изложение ответа.

«4» (хорошо) – если обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«3» (удовлетворительно) – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«2» (неудовлетворительно) – если обучающийся имеет разрозненные, бессистемные знания, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Критерии оценивания заданий практических работ.

Практическая работа оценивается максимально оценкой «5» (отлично).

Каждое задание оценивается максимально оценкой «5» (отлично).

По результатам оценивания всех заданий оценка соответствует средней.

Критерии оценивания решений задач.

«5» (отлично) – составлен правильный алгоритм решения задачи, в логическом рассуждении, в выборе нормативных источников и решении нет ошибок, получен верный ответ, задача решена рациональным способом.

«4» (хорошо) – составлен правильный алгоритм решения задачи, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор нормативных источников; есть объяснение решения, но задача решена нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.

«3» (удовлетворительно) – задание выполнено, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе нормативных источников; задача решена не полностью или в общем виде.

«2» (неудовлетворительно) – задача решена неправильно.

Критерии оценивания заданий по составлению схемы.

«5» (отлично) – выполнены все требования по составлению схемы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность построения элементов; оформлено эстетично и аккуратно.

«4» (хорошо) – основные требования к схеме выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении.

«3» (удовлетворительно) – имеются существенные отступления от темы схемы, в частности, тема освещена частично; отсутствует логическая последовательность построения элементов; допущены фактические ошибки в содержании элементов схемы.

«2» (неудовлетворительно) – схема не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания заданий по составлению таблиц.

«5» (отлично) – выполнены все требования по составлению таблицы: логически последовательно изложен весь необходимый материал; присутствует логическая последовательность в суждениях; оформлено эстетично и аккуратно; присутствует логически верный вывод.

«4» (хорошо) – основные требования к таблице выполнены, но при этом допущены недочёты, в частности, имеются неточности в изложении материала; имеются упущения в оформлении; отсутствует логически верный вывод.

«3» (удовлетворительно) – имеются существенные отступления от темы таблицы, в частности, тема освещена частично; допущены фактические ошибки в содержании; отсутствует логическая последовательность в суждениях; отсутствует вывод.

«2» (неудовлетворительно) – таблица не завершена, обнаруживается существенное непонимание ее темы.

Критерии оценивания тестовых заданий.

«5» (отлично) – 30 верных ответов (100%).

«4» (хорошо) – 22-29 верных ответов (75%-95%).

«3» (удовлетворительно) – 15-21 верных ответов (50%-70%).

«2» (неудовлетворительно) – менее 15 верных ответов (менее 50%).

Критерии оценивания тестовых заданий контрольных работ.

«5» (отлично) – 30 верных ответов (100%).

«4» (хорошо) – 22-29 верных ответов (75%-95%).

«3» (удовлетворительно) – 15-21 верных ответов (50%-70%).

«2» (неудовлетворительно) – менее 15 верных ответов (менее 50%).