

Паспорт

оценочных материалов для проведения текущего контроля и
промежуточной аттестации обучающихся по дисциплине (модулю)
«Информационная безопасность в профессиональной деятельности»

Перечень оценочных материалов и индикаторов достижения компетенций,
сформированность которых они контролируют

Наименование оценочного средства	Коды индикаторов достижения формируемых компетенции	Номер приложения
Тесты	ИД-1 _{УК-1} ИД-2 _{УК-1} ИД-3 _{УК-1}	1
Зачет	ИД-1 _{УК-1} ИД-2 _{УК-1} ИД-3 _{УК-1}	2

Утверждено на заседании кафедры «Вычислительная техника»

протокол № 3 от «11» 10 2021 года

Заведующий кафедрой  К. В. Святков

I. Текущий контроль

Приложение 1

Тесты

1. Процедура проведения тестирования

Количество проводимых тестов в течение всего периода освоения дисциплины	5 тестов
Общее количество тестовых вопросов в банке тестов	50 вопросов
Количество задаваемых тестовых вопросов в одном тесте	10 вопросов
Формат проведения тестирования	Электронный
Сроки / Периодичность проведения тестирования	После изучения каждого раздела дисциплины

2. Шкала оценивания с учетом срока сдачи

Количество правильных ответов / Процент правильных ответов	Балл
10/100	Отлично
8/80 и более	Хорошо
6/60 и более	Удовлетворительно
Менее 6/60	Неудовлетворительно

3. Тестовые задания

Тестовые задания по разделу «Обеспечение информационной безопасности в банковской сфере»

Тест №1

Онлайн-сервис, позволяющий гражданам приобретать финансовые продукты от разных организаций на одной платформе – это:

- а) блокчейн
- б) маркетплейс**
- в) Big Data
- г) мастерчейн

Тест №2

Чтобы сделать перевод в системе быстрых платежей (СБП) необходимо указать:

- а) номер телефона получателя**
- б) номер карты получателя
- в) номер счета получателя
- г) банк, на счет в котором нужно перевести деньги**

Тест №3

Технологии, используемые для упрощения выполнения финансовыми организациями требований Банка России – это:

- a) SupTech
- б) RegTech**
- в) Top-down
- г) KYC

Тест №4

Какие биометрические персональные данные позволяют физическим лицам в РФ получать банковские услуги с помощью удаленной идентификации?

- а) изображение лица**
- б) изображение радужной оболочки глаза
- в) отпечатки пальцев
- г) голос

Тест №5

Какой инструмент лидирует при хищениях денежных средств со счетов граждан?

- а) кардинг
- б) вредоносное ПО
- в) фишинг
- г) социальная инженерия**

Тест №6

К свойствам эффективно работающей автоматизированной информационной системы банка относятся:

- а) доступность**
- б) целостность**
- в) конфиденциальность**
- г) анонимность

Тест №7

Объектами безопасности коммерческого банка являются:

- а) служба безопасности
- б) персонал**
- в) информационные ресурсы**
- г) финансовые средства**

Тест №8

Угрозы информационным ресурсам коммерческого банка непосредственно осуществляются через:

- а) невозврат кредитных ссуд
- б) подкуп или шантаж сотрудников банка**
- в) подлог платежных документов
- г) неофициальный доступ и съем конфиденциальных данных**

Тест №9

Защита информации при помощи её шифрования – это:

- а) организационная защита
- б) техническая защита
- в) физическая защита
- г) криптографическая защита**

Тест №10

К киберрискам банковской системы относятся:

- а) коммерческий подкуп сотрудников и руководителей
- б) нарушение надежности и непрерывности предоставления финансовых услуг**
- в) угроза несанкционированного физического доступа
- г) хищение средств клиентов финансовых организаций

Тестовые задания по разделу «Нормативно-правовая база защиты информации в банковской сфере»

Тест №1

Под понятие банковской тайны в РФ попадает:

- а) информация о тарифах по банковским продуктам
- б) штатное расписание банка
- в) информация о операциях своих клиентов**
- г) информация о вкладах корреспондентов

Тест №2

Положения стандарта Банка России СТО БР ИББС-1.0-2014:

- а) применяются полностью на добровольной основе
- б) применяются полностью на обязательной основе
- в) утратили силу
- г) применяются на добровольной основе, за исключением положений обязательность применения, которых установлена законодательством РФ**

Тест №3

Кто, согласно СТО БР ИББС-1.0-2014 обладает наибольшими возможностями для нанесения ущерба банковской системе?

- а) собственный персонал банков**
- б) российские киберпреступники
- в) зарубежные киберпреступники
- г) клиенты и контрагенты банков

Тест №4

Согласно СТО БР ИББС-1.0-2014 наиболее актуальными источниками угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений являются:

- а) внутренние нарушители информационной безопасности: администраторы серверов**
- б) внутренние нарушители информационной безопасности: представители менеджмента организации
- в) внутренние нарушители информационной безопасности: пользователи банковских приложений
- г) несоответствие требованиям надзорных и регулирующих органов

Тест №5

Какую ответственность предполагает разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей?

- а) административную
- б) гражданско-правовую**

- в) дисциплинарную
- г) уголовную

Тест №6

Согласно ГОСТ Р 57580.1-2017 сохранение целостности и неизменности информации путем дублирования действий субъектов доступа в рамках реализации финансовых операций до их окончательного завершения – это:

- а) многофакторная аутентификация
- б) двухсторонняя аутентификация
- в) инцидент защиты информации
- г) «двойное управление»

Тест №7

Согласно ГОСТ Р 57580.2-2018 оценку соответствия защиты информации следует основывать на свидетельствах, полученных из:

- а) опросов клиентов проверяемой организации
- б) **опросов сотрудников проверяемой организации**
- в) опросов контрагентов проверяемой организации

Тест №8

В каких случаях ГОСТ Р 57580.1-2017 предусматривает возможность применения компенсационных (не входящих в базовый состав документа) мер защиты информации?

- а) низкий операционный риск
- б) участие в системе ФинЦЕРТ
- в) **отсутствие экономической целесообразности**
- г) **невозможность технической реализации**

Тест №9

Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа ГОСТ Р 57580.1-2017 включает контроль отсутствия незаблокированных учетных записей:

- а) **уволенных работников**
- б) работников внешних (подрядных) организаций
- в) работников, отсутствующих на рабочем месте от 30 календарных дней
- г) временно нетрудоспособных работников

Тест №10

В каких случаях Банк России вправе потребовать от кредитной организации передачу на хранение резервных копий баз данных?

- а) высокий операционный риск
- б) **введение запрета на привлечение во вклады денежных средств**
- в) приобретение контрольного пакета кредитной организации иностранным физическим лицом
- г) приобретение контрольного пакета кредитной организации иностранным юридическим лицом.

Тестовые задания по разделу «Цифровая инфраструктура обеспечения информационной безопасности в банковской сфере»

Тест №1

Свойство информации, в рамках функционирующей автоматической системы обработки информации (АСОИ), находиться в неискаженном виде – это:

- а) доступность
- б) целостность**
- в) конфиденциальность
- г) безопасность

Тест №2

К внутренней безопасности автоматической системы обработки информации (АСОИ) относится:

- а) защита от техногенных чрезвычайных ситуаций
- б) защита от чрезвычайных ситуаций природного характера
- в) обеспечение своевременного обслуживания поступающих запросов**
- г) защита от проникновения злоумышленников

Тест №3

Примером реализации какого подхода к обеспечению безопасности АСОИ являются автономные системы шифрования?

- а) фрагментарного**
- б) комплексного
- в) организационного

Тест №4

Классификации информационных систем (ИС) по архитектуре предполагает наличие:

- а) автоматизированных и автоматических ИС
- б) поисковых и решающих ИС
- в) управляющих и советующих ИС
- г) файл-серверных и клиент-серверных ИС**

Тест №5

Недостаток использования естественного языка в качестве информационно-поискового предполагающий наличие слов одинаковых по написанию, но разных по смыслу - это:

- а) синонимия
- б) многозначность**
- в) эллипсность
- г) парадигматические отношения между словами

Тест №6

В какой информационной системе (ИС) база данных и система управления базами данных находится на сервере, а клиентские приложения находятся на рабочих станциях?

- а) локальной ИС
- б) файл-серверной ИС
- в) клиент-серверной ИС**

Тест №7

Какой из основных прикладных процессов АСОИ ФинЦЕРТ предполагает поддержку процедур реагирования и расследования?

- а) получение информации (данных) от Участника
- б) передача информации (данных) Участнику
- в) проведение мониторинга информационных ресурсов Интернет
- г) обработка информации о компьютерных атаках**

Тест №8

Действия при выявлении операций, соответствующих признакам операций без согласия включают:

- а) предоставление клиенту информации об операции**
- б) предоставление клиенту рекомендаций по снижению риска**
- в) запрос подтверждения операции**
- г) перевод денег клиента на безопасный счет

Тест №9

Вредоносное программное обеспечение для шифрования файлов и последующего требования выкупа устанавливается на компьютер пользователей при помощи:

- а) вложений писем**
- б) фишинга
- в) телефонных звонков
- г) кардинга

Тест №10

Открытые потоки данных с индикаторами компрометации которые можно использовать для выявления и пресечения деятельности мошенников – это:

- а) вендоры
- б) фиды**
- в) REST API
- г) фрод
- д) cookie

Тестовые задания по разделу «Технические средства противодействия угрозам информационной безопасности в банковской сфере»

Тест №1

Требования к абсолютно стойким системам шифрования К. Шеннона включают:

- а) каждый ключ используется на регулярной основе множество раз
- б) ключ статистически надёжен**
- в) длина ключа должна быть меньше длины сообщения

Тест №2

В случае если для зашифровывания и расшифровывания используется два разных ключа, речь идет об:

- а) алфавитном алгоритме шифрования
- б) симметричном шифровании
- в) асимметричном шифровании**

Тест №3

Что используется для шифрования аутентификационной информации?

- а) главный ключ (мастер – ключ)
- б) ключи для шифрования ключей
- в) ключи для шифрования данных**

Тест №4

Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом – это:

- а) простая электронная подпись**
- б) неквалифицированная электронная подпись
- в) квалифицированная электронная подпись

Тест №5

Кто может обратиться за услугой по выдаче квалифицированной электронной подписи в Удостоверяющий центр ФНС России?

- а) кредитные организации
- б) операторы платежных систем
- в) должностные лица государственных органов
- г) нотариусы**

Тест №6

Какой фактор улучшает скоринг-балл в кредитном отчете?

- а) наличие иждивенцев
- б) кредиты, проданные коллекторам
- в) отсутствие кредитов**
- г) «серая» заработная плата

Тест №7

В каких целях банки используют кластеры Big Data?

- а) начисления заработной платы сотрудникам
- б) составления и подачи исковых заявлений в суд
- в) создание персонифицированных предложений клиентам**
- г) автоматического выявления мошеннических операций**

Тест №8

По какой причине Сбербанк потерял миллиарды рублей при использовании технологий искусственного интеллекта (ИИ)?

- а) обработка больших объемов данных с малой ошибкой алгоритма**
- б) гендерная дискриминация и расизм самообучающегося алгоритма ИИ
- в) ошибки системы распознавания лиц
- г) уязвимость ИИ к кибератакам
- д) коммерческий подкуп

Тест №9

Технические меры борьбы с киберзлоумышленниками включают:

- а) социальную инженерию
- б) инспектирование портов USB**
- в) баскет-метод
- г) контроль учетных записей**

Тест №10

Найдите утилиту, необходимую для работы программного комплекса, проверяющего подлинность электронной отчетности, предоставляемой в кредитные организации.

- а) КриптоПро CSP**
- б) WinToUSB
- в) Tunngle
- г) CoinVaultDecryptor
- д) Госуслуги

Тестовые задания по разделу «Кадровая составляющая противодействия угрозам информационной безопасности в банковской сфере»

Тест №1

К угрозам кадровой безопасности относятся:

- а) спуфинг
- б) профессиональная некомпетентность**
- в) нарушение контрольно-пропускного режима
- г) сбой в работе сигнализации
- д) ротация кадров

Тест №2

Какие оперативные методы вправе использовать работодатель при работе с персоналом?

- а) видеонаблюдение на рабочем месте**
- б) проверка служебной почты**
- в) проверка личной почты при помощи ей взлома, если переписка велась с рабочего компьютера
- г) проверка личной почты при помощи программ мониторинга интернет-трафика и активности пользователей, если переписка велась с рабочего компьютера**

Тест №3

Выполнить проверку соискателя на должность по списку недействительных российских паспортов можно в базе:

- а) МВД РФ**
- б) ФСБ РФ
- в) Минкомсвязи РФ
- г) Государственной автоматизированной системы РФ «Правосудие»

Тест №4

Что не является компонентом корпоративной культуры?

- а) принятая система лидерства
- б) стиль разрешения конфликтов
- в) действующая система коммуникации
- г) учредительные документы**
- д) принятая символика

Тест №5

Какие последствия могут ждать сотрудника в случае доказательства его вины по результатам служебного расследования?

- а) дисциплинарная ответственность**
- б) взыскание упущенной выгоды
- в) взыскание прямого действительного ущерба**
- г) взыскание репутационного ущерба

Тест №6

Метод проверки эффективности службы безопасности при котором её сотрудники могут начать искусственно создавать нарушения:

- а) метод «учебной тревоги»
- б) оценка количества раскрытых нарушений**
- в) оценка по успеху-неудачам организации
- г) экспертный метод
- д) метод соблюдения регламентов

Тест №7

Метод оценки персонала посредством наблюдения его поведения в моделируемых деловых ситуациях – это:

- а) ассесмент-центр**
- б) метод «360 градусов»
- в) тестирование
- г) метод КРІ
- д) exit-интервью

Тест №8

Согласно психогенетическим исследованиям, реакции людей на факторы, вызывающие стресс:

- а) практически полностью определяются генетической предрасположенностью
- б) практически полностью определяются воспитанием, жизненным опытом и тренировками
- в) на 30-40% определяются генами, полученными от родителей, и на 60-70% зависят от воспитания, опыта, навыков и тренировок**
- г) на 30-40% определяются воспитанием, жизненным опытом, навыками и тренировками, и на 60-70% зависят от родительских генов.

Тест №9

Технология подбора эксклюзивных сотрудников среди работающих специалистов других компаний - это:

- а) скрининг
- б) executive search**
- в) preliminarining
- г) френдхантинг

Тест №10

Какой вид мотивации сотрудников должен быть первичным согласно иерархической модели потребностей человека А. Маслоу?

- а) материальная мотивация**
- б) социальная мотивация
- в) психологическая мотивация
- г) духовная мотивация

II. Промежуточная аттестация

Приложение 2

Зачет

1. Процедура проведения

Общее количество вопросов к зачету	24 вопроса
Формат проведения	Устно

2. Шкала оценивания с учетом текущего контроля работы обучающегося в семестре

Критерии оценки уровня сформированности компетенций по дисциплине	Балл
Выставляется обучающемуся, если он показал знание материала по поставленному вопросу, грамотно и логично излагает его содержание, не допускает грубых ошибок в ответе на поставленный вопрос	Зачтено
Выставляется обучающемуся, если он не показал знание материала по поставленному вопросу и не может грамотно и логично изложить его содержание, допускает грубые ошибки в ответе на поставленный вопрос	Не зачтено

3. Вопросы к зачету

1. Направления и инструменты цифровой трансформации банковской системы
2. Система комплексной безопасности коммерческого банка и её информационная составляющая
3. Основные направления защиты информации в кредитно-финансовой сфере
4. Особенности правового регулирования банковской тайны в РФ
5. Сущность СТО БР ИББС-1.0 и его значение для защиты информации в банковской сфере
6. Сущность и значение национальных стандартов безопасности банковских и финансовых операций
7. Киберпреступность: современное состояние проблемы
8. Роль АСОИ ФинЦЕРТ в обеспечении безопасности банковской системы
9. Противодействие финансовым операциям без согласия клиента
10. Угрозы безопасности автоматизированных банковских систем
11. Методология защиты автоматизированных банковских систем
12. Симметричное и асимметричное шифрование в обеспечении информационной безопасности

13. Национальные и межгосударственные стандарты в сфере криптографической защиты информации
14. Практическая реализация технологии цифровой подписи: проблемы и перспективы
15. Искусственный интеллект и Big Data в информационной безопасности банков
16. Программные инструменты противодействия внутреннему мошенничеству
17. Программные инструменты противодействия внешнему мошенничеству
18. Особенности и механизм подбора сотрудников и руководителей в кредитно-финансовой сфере
19. Основные угрозы в области кадровой безопасности банка
20. Обеспечение безопасности банка при увольнении сотрудника
21. Механизмы и инструменты повышение эффективности работы персонала банка
22. Выявление фактов противоправных действий и внутренние служебные расследования в коммерческом банке
23. Роль корпоративной культуры в обеспечении безопасности банков
24. Взаимодействие службы безопасности банка с государственными и негосударственными структурами