МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Костромская государственная сельскохозяйственная академия»

Утверждаю:
Декан экономического факультета
Надежда Александровна Середа Подписано цифровой подписью: Надежда Александровна Середа Дата: 2023.06.14 16:49:31 +03'00' / Середа Н.А. /
14 июня 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

Направление подготовки (специальность) ВО	38.03.01 «Экономика»
Направленность (специализация)/ профиль	«Экономическая безопасность»
Квалификация выпускника	бакалавр
Форма обучения	очная
Срок освоения ОПОП ВО	4 года

Караваево 2023

Фонд оценочных средств предназначен для оценивания сформированности компетенций по дисциплине «Информационная безопасность в цифровой экономике»

Разработчик:
заведующий кафедрой бухгалтерского учета
и информационных систем в экономике

Обенко О.Т. _____

Подписано цифровой подписью:
Ольга Тихоновна Обенко
Дата: 2023.04.29 15:05:42 +03'00'

Утвержден на заседании кафедры «Бухгалтерский учет и информационные системы в экономике», протокол № 10 от 29.04.2023.

Заведующий кафедрой Обенко О.Т. _____

Подписано цифровой подписью: Ольга Тихоновна Обенко
Дата: 2023.04.29 15:06:05 +03'00'

Согласовано:
Председатель методической комиссии экономического факультета

Королева Е.В.
протокол № 3 от 07.06.2023 _____

Елена Владимировна Королёва

Подписано цифровой подписью: Елена Владимировна Королёва
Дата: 2023.06.07 15:10:49 +03'00'

Паспорт фонда оценочных средств

Таблица 1

Модуль дисциплины	Формируемые компетенции или их части	Оценочные материалы и средства	Количество
Основы информационной безопасности	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач ПКос-5. Способен разрабатывать мероприятия по воздействию на риск в разрезе отдельных видов и проводить их экономическую оценку	Опрос Тестирование	15 28
Концептуальные основы защиты информации		Опрос Тестирование	25 60
Нормативно-правовые аспекты информационной безопасности и защиты информации		Опрос Тестирование	20 35
Организация системы защиты информации в информационных системах		Опрос ИДЗ Тестирование	25 145

1 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ ДЕЯТЕЛЬНОСТИ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 2 – Формируемые компетенции

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (части компетенции)	Оценочные материалы и средства
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач ПКос-5. Способен разрабатывать мероприятия по воздействию на риск в разрезе отдельных видов и проводить их экономическую оценку	**Модуль 1** Основы информационной безопасности	
	ИД-1$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2$_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3$_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4$_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	Опрос Тестирование
	Модуль 2 Концептуальные основы защиты информации	
	ИД-1$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2$_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3$_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4$_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	Опрос Тестирование
	Модуль 3 Нормативно-правовые аспекты информационной безопасности и защиты информации	
	ИД-1$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2$_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3$_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки	Опрос Тестирование

	ИД-4$_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	
	Модуль 4 Организация системы защиты информации в информационных системах	
	ИД-1$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2$_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3$_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4$_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	Опрос ИДЗ Тестирование

Оценочные материалы и средства для проверки сформированности компетенций

Модуль 1. Основы информационной безопасности

Вопросы для устного опроса:

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
5. Что такое концепция информационной безопасности?
6. Что такое доктрина информационной безопасности?
7. Какие вопросы отражаются в Концепции информационной безопасности?
8. Информационная безопасность в условиях функционирования в России глобальных сетей.
9. Что такое конфиденциальная информация?
10. Назовите информационные угрозы для государства.
11. Какие создаются информационные угрозы для компании?
12. Что угрожает личности (физическому лицу)?
13. Назовите причины информационных угроз.
14. Какие действия и события нарушают ИБ?
15. Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ?

Компьютерное тестирование (ТСк)

Выберите один правильный вариант ответа

«Под информационной безопасностью будем понимать защищенность информации и …….. от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам

информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»

поддерживающей инфраструктуры

человека

+конфиденциальных данных

Защита информации – это …

комплекс мероприятий, направленных на обеспечение информационной безопасности

совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

+все определения корректны

Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба, называются:

+обнаружение угроз

пресечения и локализация угроз

ликвидация угроз

Возможность за приемлемое время получить требуемую информационную услугу называется:

+доступностью информации

целостностью информации

предоставлением информации

Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

+доступностью информации

целостностью информации

предоставлением информации

конфиденциальностью информации

Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации

доступность информации

+целостность информации

предоставление информации

конфиденциальность информации

Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:

законодательного уровня

+административного уровня

процедурного уровня

программно-технического уровня

программно-аппаратного уровня

Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?

ISO

ITU

ANSI
NIST
+NASA
SWIFT
GISA

Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:

+Федеральная служба по техническому и экспортному контролю при Президенте РФ
Федеральная служба безопасности Российской Федерации
Служба внешней разведки Российской Федерации

Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:

+Политикой безопасности
методами защиты информации
ограничением доступа к информации
учетными записями пользователей

Потенциальная возможность определенным образом нарушить информационную безопасность – это ….

+угроза
атака
взлом

Источниками угрозы называют …

+потенциальных злоумышленников
компьютерные вирусы
глобальную сеть Интернет

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …

окном безопасности
окном опасности
скользящим окном
+окном угрозы

Ошибки программного обеспечения с точки зрения информационной безопасности являются:

+уязвимым местом
окном опасности
окном безопасности
источником угрозы

Ошибки администрирования системы с точки зрения информационной безопасности являются:

уязвимым местом
+окном опасности
окном безопасности
источником угрозы

Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:

уязвимым местом
окном опасности
окном безопасности
+источником угрозы

Некоторая уникальная информация, позволяющая различать пользователей называется:

+идентификатор (логин)
пароль
учетная запись
ключ

Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:

идентификатор (логин)
+пароль
учетная запись
ключ

Совокупность идентификатора и пароля пользователя называется:

логин пользователя
+учетная запись пользователя
ключ пользователя

Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:

+идентификацией пользователя
аутентификацией пользователя
опознанием пользователя
созданием учетной записи пользователя

Проверка принадлежности пользователю предъявленного им идентификатора является:

идентификацией пользователя
+аутентификацией пользователя
регистрацией пользователя
созданием учетной записи пользователя

Факт получения охраняемых сведений злоумышленниками или конкурентами называется:

утечкой
разглашением
+взломом

Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:

+утечкой
разглашением
взломом

Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена называется:

утечкой
+разглашением
взломом

Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:

+«Отказ от обслуживания» (Denial of Service - DoS)
Срыв стека
Внедрение на компьютер деструктивных программ
Перехват передаваемой по сети информации (Sniffing)
Спуфинг

Сканирование портов

Атака, целью которой является трафик локальной сети, называется:

«Отказ от обслуживания» (Denial of Service - DoS)

Срыв стека

Внедрение на компьютер деструктивных программ

+Снифинг (Sniffing)

Спуфинг

Сканирование портов

Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:

«Отказ от обслуживания» (Denial of Service - DoS)

Срыв стека

Внедрение на компьютер деструктивных программ

Снифинг (Sniffing)

+Спуфинг

Сканирование портов

Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:

«Отказ от обслуживания» (Denial of Service - DoS)

Срыв стека

Внедрение на компьютер деструктивных программ

Снифинг (Sniffing)

Спуфинг

+Сканирование портов

Таблица 3 – Критерии оценки сформированности компетенций

Код и наименование индикатора достижения компетенции (части компетенции)	Критерии оценивания сформированности компетенции (части компетенции)
	соответствует оценке «зачтено» 50-100% от максимального балла
ИД-1-$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2- $_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3- $_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4- $_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов	владеет материалом по теме, но допускает неточности при формулировке основных понятий, в основном правильно анализирует задачу, выделяя ее базовые составляющие; достаточно эффективно осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи; планирует возможные варианты решения задачи, оценивая их достоинства и недостатки; достаточно полно определяет и оценивает последствия возможных решений задачи, определяет источники информации на основе поставленных целей для решения экономических задач; не вполне уверенно определяет методы сбора, обработки

ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	информации, способы и вид ее представления; разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов, может допускать неточности при проведении экономическую оценку мероприятий по воздействию на риск, что не оказывает существенного влияния на общий уровень сформированности компетенций.

Модуль 2. «Концептуальные основы защиты информации

1. Вопросы для устного опроса:

1. Перечислите виды защищаемой информации.
2. Какие методы защиты информации выделяют?
3. Что такое правовые методы защиты информации?
4. Что такое организационные методы защиты информации?
5. Что такое технические методы защиты информации?
6. Что такое программно-аппаратные методы защиты информации?
7. Что такое криптографические методы защиты информации?
8. Что такое физические методы защиты информации?
9. Назовите основные принципы политики безопасности.
10. Что включает политика безопасности верхнего уровня?
11. Как организован удаленный доступ к сервису?
12. Что включает политика управления паролями?
13. Как оценить риски реализации угроз информации?
14. Какие этапы выделяются в жизненном цикле информационного сервиса?
15. На каких принципах базируется системный подход к защите информации?
16. Как обеспечивается управление доступом?
17. Какие программные средства используются для ИБ?
18. В чем отличия метода принуждения от метода побуждения?
19. Что такое электронная подпись и для чего она используется?
20. Понятие криптографии шифра.
21. Задачи и методы криптографии.
22. Виды шифров.
23. Криптографические примитивы.
24. Основные криптографические протоколы.
25. Модели основных криптоаналитических атак.

Компьютерное тестирование (ТСк)

Выберите один правильный вариант ответа

Дублирование сообщений является угрозой:
доступности;
конфиденциальности;
+целостности.
Вредоносное ПО Melissa подвергает атаке на доступность:
системы электронной коммерции;

геоинформационные системы;
+системы электронной почты.

Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

+Melissa.
Bubble Boy.
ILO VE YOU.

Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

просчеты при администрировании информационных систем;
необходимость постоянной модификации информационных систем;
+сложность современных информационных систем.

Агрессивное потребление ресурсов является угрозой:

+доступности
конфиденциальности
целостности

Программа Melissa — это:

бомба;
+вирус;
червь.

Для внедрения бомб чаще всего используются ошибки типа:

отсутствие проверок кодов возврата;
+переполнение буфера;
нарушение целостности транзакций.

Окно опасности появляется, когда:

становится известно о средствах использования уязвимости;
+появляется возможность использовать уязвимость;
устанавливается новое ПО.

Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:

средства выявления злоумышленной активности;
средства обеспечения отказоустойчивости;
+средства контроля эффективности защиты информации.

Уровень безопасности В согласно «Оранжевой книге» характеризуется:

произвольным управлением доступом;
+принудительным управлением доступом;
верифицируемой безопасностью.

Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы:

периметр безопасности;
+метки безопасности;
сертификаты безопасности.

Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:

управление квотами;
+управление доступом;
экранирование.

Уровень безопасности А согласно «Оранжевой книге» характеризуется:

произвольным управлением доступом;
принудительным управлением доступом;
+верифицируемой безопасностью.

Согласно рекомендациям X.800 аутентификация может быть реализована на:

+сетевом уровне;
транспортном уровне;
прикладном уровне.

В число целей политики безопасности верхнего уровня входят:

+управление рисками;

определение ответственных за информационные сервисы;

определение мер наказания за нарушения политики безопасности.

Политика безопасности строится на основе:

общих представлений об ИС организации;

изучения политик родственных организаций;

+анализа рисков.

В число целей политики безопасности верхнего уровня входят:

+формулировка административных решений по важнейшим аспектам реализации программы безопасности;

выбор методов аутентификации пользователей;

обеспечение базы для соблюдения законов и правил.

Риск является функцией:

+размера возможного ущерба;

числа пользователей информационной системы;

уставного капитала организации.

Первый шаг в анализе угроз — это:

+ идентификация угроз;

аутентификация угроз;

ликвидация угроз.

Оценка рисков позволяет ответить на следующие вопросы:

+чем рискует организация, используя информационную систе му?

чем рискуют пользователи информационной системы?

чем рискуют системные администраторы?

В число принципов управления персоналом входят:

+минимизация привилегий;

минимизация зарплаты;

максимизация зарплаты.

Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

+выработка и проведение в жизнь единой политики безопасности;

унификация аппаратно-программных платформ;

минимизация числа используемых приложений.

Экранирование может использоваться для:

+предупреждения нарушений И Б;

обнаружения нарушений;

локализации последствий нарушений.

В число основных принципов архитектурной безопасности входят:

+следование признанным стандартам;

применение нестандартных решений, не известных злоумышленникам;

разнообразие защитных средств.

Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

использование собственных линий связи;

+обеспечение конфиденциальности и целостности при сетевых взаимодействиях;

полный анализ сетевого трафика.

В число универсальных сервисов безопасности входят:

+ управление доступом;

управление информационными системами и их компонентами;

управление носителями.

Контроль целостности может использоваться для:

предупреждения нарушений И Б;

+обнаружения нарушений;

локализации последствий нарушений.

В качестве аутентификатора в сетевой среде могут использоваться:

кардиограмма субъекта;

номер карточки пенсионного страхования;

+результат работы генератора одноразовых паролей.

В число основных понятий ролевого управления доступом входит:

+роль;

исполнитель роли;

пользователь роли.

В качестве аутентификатора в сетевой среде могут использоваться:

год рождения субъекта;

фамилия субъекта;

+секретный криптографический ключ.

Ролевое управление доступом использует следующее средство объектно-ориентированного подхода:

инкапсуляция;

+наследование;

полиморфизм.

Цифровой сертификат содержит:

+открытый ключ пользователя;

секретный ключ пользователя;

имя пользователя.

Криптография необходима для реализации следующих сервисов безопасности:

идентификация;

экранирование;

+аутентификация.

Криптография необходима для реализации следующих сервисов безопасности:

+контроль конфиденциальности;

контроль целостности;

контроль доступа.

Экран выполняет функции:

+разграничения доступа;

облегчения доступа;

усложнения доступа.

Демилитаризованная зона располагается:

перед внешним межсетевым экраном;

+между межсетевыми экранами;

за внутренним межсетевым экраном.

Экранирование на сетевом и транспортном уровнях может обеспечить:

+ разграничение доступа по сетевым адресам;

выборочное выполнение команд прикладного протокола;

контроль объема данных, переданных по TCP-соединению.

Системы анализа защищенности помогают предотвратить:

+известные атаки;

новые виды атак;

нетипичное поведение пользователей.

Среднее время наработки на отказ:

пропорционально интенсивности отказов;

+обратно пропорционально интенсивности отказов;

не зависит от интенсивности отказов.

Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели 081:

+сетевом;

сеансовом;

уровне представления.

Принцип усиления самого слабого звена можно переформулировать как:

+принцип равнопрочности обороны;

принцип удаления слабого звена;

принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь.

Политика безопасности:

фиксирует правила разграничения доступа;

+отражает подход организации к защите своих информационных активов;

описывает способы защиты руководства организации.

Выберите несколько правильных вариантов ответа

При анализе стоимости защитных мер следует учитывать:

+расходы на закупку оборудования;

+расходы на закупку программ;

+расходы на обучение персонала;

упущенную выгоду.

В число основных понятий ролевого управления доступом входит:

+объект;

+субъект;

метод.

Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:

перехвата;

+воспроизведения;

+атак на доступность.

В число универсальных сервисов безопасности входят:

средства построения виртуальных локальных сетей;

+экранирование;

+протоколирование и аудит.

В число основных принципов архитектурной безопасности входят:

+усиление самого слабого звена;

укрепление наиболее вероятного объекта атаки;

+эшелонированность обороны.

Протоколирование и аудит могут использоваться для:

+предупреждения нарушений И Б;

+обнаружения нарушений;

восстановления режима И Б.

В число этапов процесса планирования восстановительных ра бот входят:

+выявление критически важных функций организации;

+определение перечня возможных аварий;

проведение тестовых аварий.

В число направлений повседневной деятельности на процедур ном уровне входят:

+ситуационное управление;

+конфигурационное управление;

оптимальное управление.

В число классов мер процедурного уровня входят:

+поддержание работоспособности;

поддержание физической формы;

+физическая защита.

Управление рисками включает в себя следующие виды деятельности:

определение ответственных за анализ рисков;

+оценка рисков;

+выбор эффективных защитных средств.

В число этапов управления рисками входят:
+идентификация активов;
ликвидация пассивов;
+ выбор объектов оценки.
В рамках политики безопасности нижнего уровня осуществляются:
стратегическое планирование;
+повседневное администрирование;
+отслеживание слабых мест защиты.
В число целей политики безопасности верхнего уровня входят:
+решение сформировать или пересмотреть комплексную программу безопасности;
+обеспечение базы для соблюдения законов и правил;
обеспечение конфиденциальности почтовых сообщений.
В число классов требований доверия безопасности «Общих критериев» входят:
+разработка;
+оценка профиля защиты;
сертификация.
Среди ниже перечисленных отметьте две троянские программы:
I LOVE YOU;
+Back Orifice;
+Netbus.
Уголовный кодекс РФ не предусматривает наказания за:
создание, использование и распространение вредоносных программ;
+ведение личной корреспонденции на производственной технической базе;
+нарушение правил эксплуатации информационных систем.
Самыми опасными источниками внутренних угроз являются:
+некомпетентные руководители;
+обиженные сотрудники;
любопытные администраторы.
В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
+ меры обеспечения целостности;
административные меры;
+ меры обеспечения конфиденциальности.

Таблица 4 – Критерии оценки сформированности компетенций

Код и наименование индикатора достижения компетенции (части компетенции)	Критерии оценивания сформированности компетенции (части компетенции)
	соответствует оценке «зачтено» 50-100% от максимального балла
ИД-1-$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2- $_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3- $_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки	владеет материалом по теме, но допускает неточности при формулировке основных понятий, в основном правильно анализирует задачу, выделяя ее базовые составляющие; достаточно эффективно осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи; планирует возможные варианты решения задачи, оценивая их достоинства и недостатки;

ИД-4- $_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	достаточно полно определяет и оценивает последствия возможных решений задачи, определяет источники информации на основе поставленных целей для решения экономических задач; не вполне уверенно определяет методы сбора, обработки информации, способы и вид ее представления; разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов, может допускать неточности при проведении экономическую оценку мероприятий по воздействию на риск, что не оказывает существенного влияния на общий уровень сформированности компетенций.

Модуль 3. «Нормативно-правовые аспекты информационной безопасности и защиты информации»

1. Вопросы для устного опроса:

1. Охарактеризуйте правовые аспекты защиты информации
2. Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности.
3. Назовите основные направления развития законодательства в области обеспечения информационной безопасности, определенные Межведомственной комиссией Совета Безопасности РФ по информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое коммерческая тайна?
10. Что такое режим коммерческой тайны?
11. Что такое государственная тайна?
12. Опишите правовой режим государственной тайны.
13. ФЗ-63.
14. Какие главные государственные органы в области обеспечения информационной безопасности?
15. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
16. Какие основные международные стандарты в области информационной безопасности?
17. Расскажите в чем суть "оранжевой книги" (ISO 15408).
18. Как связаны международные стандарты и стандарты РФ?
19. Какие основные стандарты РФ в области информационной безопасности существуют?
20. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2012.

Компьютерное тестирование (ТСк)

Выберите один правильный вариант ответа

Предмет правового обеспечения информационной безопасности представляет собой:

+совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз;

совокупность общественных отношений, на которые направлено правовое воздействие только в целях недопущения проявлений угроз объектам национальных интересов в информационной сфере;

нет верного ответа.

Правовое обеспечение безопасности информации в форме сведений образуется:

+совокупностью норм и институтов, регулирующих отношения по поводу только объекта - сведений, обладателем которых является субъект права;

совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;

совокупностью норм и институтов, регулирующих отношения по поводу только объекта - свобода мысли.

Правовое обеспечение безопасности информации в форме сообщений определяется:

совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права;

свобода мысли; субъективная значимость национальных культурных ценностей;

+совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы;

совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации;

совокупностью правовых норм и институтов.

Содержание и структура законодательства в области информационной безопасности включает:

+Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;

Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации;

Подзаконные акты Правительства Российской Федерации – Федеральные законы - Кодексы;

нет верного ответа.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:

+Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;

Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;

Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;

Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.

Предметом правового регулирования в области информации, информационных технологий и защиты информации являются:

отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации;

отношения, возникающие только при применении информационных технологий;

отношения, возникающие только при обеспечении защиты информации;

+отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

Документированной информацией называют:

+информацию, зафиксированную на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

информацию, зафиксированную на материальном носителе путем документирования, без реквизитов;

нет верного ответа.

К общедоступной информации относятся:

общеизвестные сведения и иная информация, доступ к которой не ограничен после достижения определенного возраста;

+общеизвестные сведения и иная информация, доступ к которой не ограничен;

нет верного ответа.

Различают следующие виды информационных систем:

+государственные информационные системы, муниципальные информационные системы, иные информационные системы;

государственные информационные системы;

муниципальные информационные системы;

нет верного ответа.

Правовой режим информационных технологий включает:

порядок регулирования использования информационно-коммуникационных сетей;

перечень областей государственного регулирования в сфере применения информационных технологий;

требования к государственным информационным системам;

+верны все варианты.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

+на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

реализацию права на доступ к информации;

верны все варианты.

Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:

отнесенные к государственной тайне;

+ отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);

отнесенные к информации о прогнозах погоды;

все верны ответы.

Как называется закон, регулирующий деятельность государственной тайны на территории РФ?

«О коммерческой тайне»;

+«О государственной тайне»;

«О служебной тайне»;

«О врачебной тайне».

К информации ограниченного доступа относятся:

государственная тайна;

конфиденциальная информация;
персональные данные;
+все ответы верны

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

подтверждена подлинность электронной цифровой подписи в электронном документе;

электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

+верны все варианты.

Перечень видов деятельности в области зашиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ - "О лицензировании отдельных видов деятельности" от 24.12.94 №1418 к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание:

шифровальных средств;
защищенных систем телекоммуникаций;
программных средств;
специальных технических средств зашиты информации;
подготовка и переподготовка кадров;
+все верны варианты.

Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?

2
3
+4
5
6

Сертификации подлежат:

+средства криптографической защиты информации;
средства выявления закладных устройств и программных закладок;
защищенные технические средства обработки информации;
защищенные информационные системы и комплексы телекоммуникаций;
все вышеперечисленные средства.

В руководящем документе Гостехкомиссии системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности – относятся к группе:

+первой;
второй;
третьей;
четвертой;
пятой.

В руководящем документе Гостехкомиссии системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности – относятся к группе:

первой;
+второй;
третьей;
четвертой;
пятой.

В руководящем документе Гостехкомиссии многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют различные права на доступ к информации – относятся к группе:

первой;
второй;
+третьей;
четвертой;
пятой.

Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

+просчеты при администрировании информационных систем
необходимость постоянной модификации информационных систем
сложность современных информационных систем

Уголовный кодекс РФ не предусматривает наказания за:

создание, использование и распространение вредоносных программ
+ведение личной корреспонденции на производственной технической базе
нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

+средства выявления злоумышленной активности
средства обеспечения отказоустойчивости
средства контроля эффективности защиты информации

В число целей политики безопасности верхнего уровня входят:

решение сформировать или пересмотреть комплексную программу безопасности
+обеспечение базы для соблюдения законов и правил
обеспечение конфиденциальности почтовых сообщений

В число целей программы безопасности верхнего уровня входят:

управление рисками
определение ответственных за информационные сервисы
+определение мер наказания за нарушения политики безопасности

В рамках программы безопасности нижнего уровня осуществляются:

стратегическое планирование
повседневное администрирование
+отслеживание слабых мест защиты

Политика безопасности строится на основе:

общих представлений об ИС организации
изучения политик родственных организаций
+анализа рисков

В число целей политики безопасности верхнего уровня входят:

формулировка административных решений по важнейшим аспектам реализации программы безопасности
выбор методов аутентификации пользователей
+обеспечение базы для соблюдения законов и правил

Действие Закона ""О лицензировании отдельных видов деятельности"" распространяется на:

деятельность по использованию шифровальных (криптографических) средств
деятельность по рекламированию шифровальных (криптографических) средств
+деятельность по распространению шифровальных (криптографических) средств

Под определение средств защиты информации, данное в Законе ""О государственной тайне", подпадают:

+средства выявления злоумышленной активности
средства обеспечения отказоустойчивости
средства контроля эффективности защиты информации

Действие Закона ""О лицензировании отдельных видов деятельности"" не распространяется на:

деятельность по технической защите конфиденциальной информации

+образовательную деятельность в области защиты информации

предоставление услуг в области шифрования информации

Под определение средств защиты информации, данное в Законе "О государственной тайне"", подпадают:

+средства выявления злоумышленной активности

средства обеспечения отказоустойчивости

средства контроля эффективности защиты информации

Что представляет собой Доктрина информационной безопасности РФ?

нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

федеральный закон, регулирующий правоотношения в области информационной безопасности;

целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

+совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Какие из перечисленных ниже угроз относятся к классу преднамеренных?

+заражение компьютера вирусами;

физическое разрушение системы в результате пожара;

отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

вскрытие шифров криптозащиты информации

Правовое обеспечение ИБ означает:

Защиту интересов физических и юридических лиц;

Защиту интересов государства и общества;

+ Все вышеперечисленное.

Таблица 5 – Критерии оценки сформированности компетенций

Код и наименование индикатора достижения компетенции (части компетенции)	Критерии оценивания сформированности компетенции (части компетенции)
	соответствует оценке «зачтено» 50-100% от максимального балла
ИД-1-$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2- $_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3- $_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4- $_{УК-1}$ Определяет и оценивает	владеет материалом по теме, но допускает неточности при формулировке основных понятий, в основном правильно анализирует задачу, выделяя ее базовые составляющие; достаточно эффективно осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи; планирует возможные варианты решения задачи, оценивая их достоинства и недостатки; достаточно полно определяет и оценивает

последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	последствия возможных решений задачи, определяет источники информации на основе поставленных целей для решения экономических задач; не вполне уверенно определяет методы сбора, обработки информации, способы и вид ее представления; разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов, может допускать неточности при проведении экономическую оценку мероприятий по воздействию на риск, что не оказывает существенного влияния на общий уровень сформированности компетенций.

Модуль 4. ***«Организация системы защиты информации в информационных системах».***

1. Вопросы для устного опроса:

1. Какие организационно-административные меры Вы знаете?
2. Назовите составляющие организационного обеспечения компьютерной безопасности.
3. Что входит в состав организационно-технических мер?
4. Перечислите организационно-экономические меры защиты информации.
5. Какие качества проверяются у лиц при приеме на работу?
6. Что включает конфиденциальное делопроизводство?
7. Для чего применяют межсетевые экраны?
8. Как классифицируются технические средства противодействия?
9. Какие подразделения в службе безопасности?
10. Какие информационные угрозы являются платой за использования Интернета?
11. Назовите меры по защите информации в интернете.
12. Для чего используются межсетевые экраны-брандмауэры?
13. Что используется для защиты электронной почты?
14. Методики обнаружения вирусов и виды антивирусного программного обеспечения.
15. Что можно использовать для защиты от вирусов?
16. Какие Вы знаете антивирусные программы?
17. Назовите основные источники проникновения вирусов.
18. Какие особенности компании необходимо учитывать при разработке системы защиты?
19. Что необходимо защищать в корпоративной сети?
20. Назовите основные этапы построения системы защиты.
21. Как классифицируют меры обеспечения безопасности по способам осуществления?
22. В чем отличия «встроенной» защиты от «добавленной»?
23. Что делается на этапе сопровождения системы?
24. Назовите критерии оптимального соотношения в анализе различных вариантов построения системы защиты.

25. Дайте характеристику плана обеспечения непрерывной работы и восстановления (ОНРВ).

Компьютерное тестирование (ТСк)

Выберите один правильный вариант ответа

"Троянский конь" является разновидностью модели воздействия программных закладок

+искажение
перехват
наблюдение и компрометация
уборка мусора

"Уполномоченные серверы" были созданы для решения проблемы

+имитации IP-адресов
подделки электронной подписи
перехвата трафика
НСД

"Уполномоченные серверы" фильтруют пакеты на уровне

+приложений
физическом
канальном
транспортном

Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни: 1) внешний; 2) сетевой; 3) клиентский; 4) серверный; 5) системный; 6) приложений

+ 1, 2, 5, 6
1, 2, 3, 4
3, 4, 5, 6
1, 3, 5, 6

ACL-список ассоциируется с каждым

+ объектом
процессом
доменом
типом доступа

_____- это выделение пользователем и администраторам только тех прав доступа, которые им необходимы

+ Принцип минимазации привилегий
Принцип максимизации привилегий
Принцип многоуровневой защиты
Принцип простоты и управляемости ИС

_____- это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные

+ Целостность
Доступность
Восстанавливаемость
Детерминированность

_____- это недостаток систем шифрования с открытым ключом

+ Относительно низкая производительность
На одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста
При использовании простой замены легко произвести подмену одного шифрованного текста другим
Необходимость распространения секретных ключей

_____- это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы

+ Авторизация
Аудит
Идентификация
Утентификация

_____- это свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов

+Конфиденциальность
Достоверность
Целостность
Детерминированность

_____- это троянские программы

+ Часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба
Программы-вирусы, которые распространяются самостоятельно
Текстовые файлы, распространяемые по сети
Все программы, содержащие ошибки

_____- это политика информационной безопасности

+Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации
Итоговый документ анализа рисков
Профиль защиты
Стандарт безопасности

_____- это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации

+Идентификация
Аутентификация
Авторизация
Аудит

_____- это проверка подлинности пользователя по предъявленному им идентификатору

+ Аутентификация
Аудит
Авторизация
Идентификация

_____- это проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы

+ Аутентификация
Авторизация
Аудит
Идентификация

_____ - цель прогресса внедрения и тестирования средств защиты

+ Гарантировать правильность реализации средств защиты
Выявить нарушителя
Определить уровень расходов на систему защиты
Выбор мер и средств защиты

_____ и т.п. с целью получения доступа к информации

+ Идентификация
Аутентификация
Авторизация
Аудит

_____- это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования

+ Безопасность информации
Уязвимость информации
Надежность информации
Защищенность информации

_____является достоинством матричных моделей безопасности

+ Легкость представления широкого спектра правил обеспечения безопасности
Контроль за потоками информации
Расширенный аудит
Гибкость управления

_____управляет регистрацией в системе Windows 2000

+ Процедура winlogon
Процедура lsass
msgina.dll
logon.dll

_____называется метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации

+ Мандатным
Избирательным
Идентифицируемым
Привилегированным

_____режим тиражирования данных улучшает рабочие характеристики системы

+ Асинхронный
Импульсный
Тоновый
Синхронный

_____создается для реализации технологии RAID

+ Псевдодрайвер
Компилятор
Интерпретатор
Специальный процесс

_____уровень ОС связан с доступом к информационным ресурсам внутри организации

+ Сетевой
Внешний
Приложений
Системный

_____является недостатком многоуровневых моделей безопасности

+ Невозможность учета индивидуальных особенностей субъекта
Отсутствие контроля за потоками информации
Сложность представления широкого спектра правил обеспечения безопасности
Отсутствие полного аудита

_____занимается обеспечением скрытности информации в информационных массивах

+ Стеганография
Криптография
Криптология
Криптоанализ

_____называется запись определенных событий в журнал безопасности сервера

+ Аудитом
Учетом

Трафиком
Мониторингом

_____называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля

+ Мониторингом
Аудитом
Администрированием
Управлением ресурсами

_____называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения

+ Электронной подписью
Идентификатором
Ключом
Шифром

_____называется процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска

+ Управлением риском
Минимизацией риска
Оптимизацией средств защиты
Мониторингом средств защиты

_____называется система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую

+ Брандмауэром
Браузером
Фильтром
Маршрутизатором

_____называется совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением

+ Качеством информации
Актуальностью информации
Доступностью
Целостностью

_____называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС

+ Программными закладками
Вирусами
Внутрипрограммными вирусами
Компьютерными червями

_____обеспечивается защита исполняемых файлов

+ Обязательным контролем попытки запуска
Дополнительным хостом
Специальным режимом запуска
Криптографией

_____обеспечивается защита от форматирования жесткого диска со стороны пользователей

+ Аппаратным модулем, устанавливаемым на системную шину ПК
Аппаратным модулем, устанавливаемым на контроллер
Специальным программным обеспечением
Системным программным обеспечением

_____определяется как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных

+ Причастность

Контроль доступа
Целостность
Аутентификация

_____уровень ОС определяет взаимодействие с глобальными ресурсами других организаций

+ Внешний
Сетевой
Приложений
Системный

_____является администратором базы данных

+ Любой пользователь, создавший БД
Системный администратор
Старший пользователь группы
Администратор сервера баз данных

_____является недостатком матричных моделей безопасности

+ Отсутствие контроля за потоками информации
Сложность представления широкого спектра правил обеспечения безопасности
Невозможность учета индивидуальных особенностей субъекта
Отсутствие полного аудита

_____является недостатком модели политики безопасности на основе анализа угроз системе

+ Изначальное допущение вскрываемости системы
Статичность
Сложный механизм реализации
Необходимость дополнительного обучения персонала

_____является содержанием параметра угрозы безопасности информации "конфиденциальность"

+ Несанкционированное получение
Несанкционированная модификация
Искажение
Уничтожение

_____являются достоинствами программной реализации криптографического закрытия данных

+ Практичность и гибкость
Высокая производительность и простота
Безопасность и эффективность
Корректность и функциональность

_____называется конечное множество используемых для кодирования информации знаков

+ Алфавитом
Шифром
Ключом
Кодом

_____называется конфигурация из нескольких компьютеров, выполняющих общее приложение

+ Кластером
Сетью
Сервером
Суперсервером

_____называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий

+ Профилем защиты
Системой защиты
Стандартом безопасности

Профилем безопасности

_____называется процесс имитации хакером дружественного адреса

+ "Спуфингом"

"Крэком"

Проникновением

Взломом

_____называется список объектов, к которым может быть получен доступ, вместе с доменом защиты объекта

+ Перечнем возможностей

Доменом

Списком управления доступом

Списком владельцев

_____называется удачная криптоатака

+ Взломом

Проникновением

Вскрытием

Раскрытием шифра

_____называется оконечное устройство канала связи, через которое процесс может передавать или получать данные

+ Сокетом

Терминалом

Хостом

Портом

_____обеспечивается защита от программных закладок

+ Аппаратным модулем, устанавливаемым на системную шину ПК

Аппаратным модулем, устанавливаемым на контроллер

Специальным программным обеспечением

Системным программным обеспечением

_____объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей

+ Криптоанализ

Криптология

Стеганография

Криптография

_____составляет основу политики безопасности

+ Способ управления доступом

Выбор каналов связи

Управление риском

Программное обеспечение

_____является достоинством модели политики безопасности на основе анализа угроз системе

+ Числовая вероятностная оценка надежности

Простой механизм реализации

Динамичность

Высокая степень надежности

_____является достоинством модели конечных состояний политики безопасности

+ Высокая степень надежности

Простота реализации

Дешевизна

Удобство эксплуатации

_____является наиболее надежным механизмом для защиты содержания сообщений

+ Криптография

Специальный аппаратный модуль

Специальный режим передачи сообщения
Дополнительный хост

_____является наукой, изучающей математические методы защиты информации путем ее преобразования

+ Криптология
Криптография
Стеганография
Криптоанализ

_____является недостатком дискретных моделей политики безопасности я

+ Статичность
Сложный механизм реализации
Изначальное допущение вскрываемости системы
Необходимость дополнительного обучения персонала

_____является недостатком модели конечных состояний политики безопасности

+ Сложность реализации
Низкая степень надежности
Статичность
Изменение линий связи

_____является первым этапом разработки системы защиты ИС

+ Анализ потенциально возможных угроз информации
Изучение информационных потоков
Стандартизация программного обеспечения
Оценка возможных потерь

_____является сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях

+ Kerberos
SendMail
Net Logon
Network DDE

_____являются достоинствами аппаратной реализации криптографического закрытия данных

+ Высокая производительность и простота
Практичность и гибкость
Доступность и конфиденциальность
Целостность и безопасность

____режим тиражирования гарантирует полную согласованность баз данных

+ Синхронный
Асинхронный
Импульсный
Тоновый

____характеризует соответствие средств безопасности решаемым задачам

+ Эффективность
Корректность
Унификация
Адекватность

____является достоинством дискретных моделей политики безопасности

+ Простой механизм реализации
Динамичность
Высокая степень надежности
Числовая вероятностная оценка надежности

____является задачей анализа модели политики безопасности на основе анализа угроз системе

+ Минимизация вероятности преодоления системы защиты
Максимизация времени взлома

Максимизация ресурса для взлома
Максимизация затрат для взлома

Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности

+ Белла-ЛаПадула
Лендвера
С полным перекрытием
На основе анализа угроз

Административные действия в СУБД позволяют выполнять привилегии

+ безопасности
доступа
чтения
тиражирования

Администратор сервера баз данных имеет имя

+ ingres
root
sysadm
admin

Администратор_____занимается регистрацией пользователей СУБД

+ сервера баз данных
сетевой
базы данных
системный

Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем

+ физическом
канальном
транспортном
сетевом

Брандмауэры второго поколения представляли собой

+ "уполномоченные серверы"
"неприступные серверы"
маршрутизаторы с фильтрацией пакетов
хосты с фильтрацией пакетов

Брандмауэры первого поколения представляли собой

+ маршрутизаторы с фильтрацией пакетов
хосты с фильтрацией пакетов
"уполномоченные серверы"
"неприступные серверы"

Брандмауэры третьего поколения используют для фильтрации

+ специальные многоуровневые методы анализа состояния пакетов
методы анализа контрольной информации
методы электронной подписи
общий анализ трафика

Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

+ доступность
детермированность
целостность
восстанавливаемость

Восстановление данных является дополнительной функцией услуги защиты

+ целостность
контроль доступа
причастность

аутентификация

Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство

+ доступность
целостность
восстанавливаемость
детерминированность

Два ключа используются в криптосистемах

+ с открытым ключом
с закрытым ключом
симметричных
двойного шифрования

Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели

+ искажение
перехват
компрометация
наблюдение

Дескриптор защиты в Windows 2000 содержит список

+ пользователей и групп, имеющих доступ к объекту
объектов, доступных пользователю и группе
привилегий, назначенных пользователю
объектов, не доступных пользователям

Длина исходного ключа в ГОСТ 28147-89 (бит)

+ 256
64
128
56

Длина исходного ключа у алгоритма шифрования DES (бит)

+ 56
256
64
128

Для решения проблемы правильности выбора и надежности функционирования средств защиты в "Европейских критериях" вводится понятие

+ адекватности средств защиты
оптимизации средств защиты
надежности защиты информации
унификации средств защиты

Для создания базы данных пользователь должен получить привилегию от

+ администратора сервера баз данных
старшего пользователя своей группы
системного администратора
сетевого администратора

Домены безопасности согласно "Оранжевой книге" используются в системах класса

+ B3
B2
C2
C3

Единственный ключ используется в криптосистемах

+ симметричных
асимметричных
с открытым ключом

с закрытым ключом

Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается

+ высокой
базовой
стандартной
сверхвысокой

Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается

+ средней
стандартной
базовой
высокой

Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается

+ базовой
средней
низкой
стандартной

Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты

+ встроенных в ОС
уровня приложений
сетевого уровня
системного уровня

Защита с применением меток безопасности согласно "Оранжевой книге" используется в системах класса

+ B1
C1
B2
C2

Идентификаторы безопасности в Windows 2000 представляют собой

+ двоичное число, состоящее из заголовка и длинного случайного компонента
строку символов, содержащую имя пользователя и пароль
число, вычисляемое с помощью хэш-функции
константу, определенную администратором для каждого пользователя

Из перечисленного аутентификация используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

+ 1, 2, 5
1, 2, 3
1, 3, 5
4, 5, 6

Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются: 1) аутентификация; 2) идентификация; 3) целостность; 4) контроль доступа; 5) контроль трафика; 6) причастность

+ 1, 3, 4, 6
1, 2, 3, 4
2, 5, 6
1, 3, 5

Из перечисленного в автоматизированных системах используется аутентификация по: 1) терминалу; 2) паролю; 3) предмету; 4) физиологическим признакам; 5) периферийным устройствам

+ 2, 3, 4
1, 2, 3

3, 4, 5

1, 2, 4

Из перечисленного в обязанности сотрудников группы информационной безопасности входят: 1) управление доступом пользователей к данным; 2) расследование причин нарушения защиты; 3) исправление ошибок в программном обеспечении; 5) устранение дефектов аппаратной части

+ 1, 2

3, 4

1, 2, 3, 4

1, 3, 4

Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы: 1) визуальное сканирование; 2) фрагментарное сканирование; 3) исследование динамических характеристик движения руки; 4) исследование траектории движения руки

+ 1, 3

1, 2

3, 4

2, 4

Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы: 1) сравнение отдельных случайно выбранных фрагментов; 2) сравнение характерных деталей в графическом представлении; 3) непосредственное сравнение изображений; 4) сравнение характерных деталей в цифровом виде

+ 3, 4

1, 2

1, 3

2, 4

Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются: 1) отпечатки пальцев; 2) форма кисти; 3) форма губ; 4) форма ушной раковины; 5) голос; 6) личная подпись

+ 1, 2, 5, 6

1, 2, 3

4, 5, 6

1, 4, 5

Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие: 1) копирование; 2) чтение; 3) запись; 4) выполнение; 5) удаление

+ 2, 3, 4

1, 2, 3

3, 4, 5

1, 2, 5

Из перечисленного для СУБД важны такие аспекты информационной безопасности, как 1) своевременность; 2) целостность; 3) доступность; 4) конфиденциальность; 5) многоплатформенность

+ 2, 3, 4

1, 2, 3

3, 4, 5

2, 4

Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как: 1) чтение; 2) удаление; 3) копирование; 4) изменение

+ 1, 4

3, 4

1, 3

2, 4

Из перечисленного защита процедур и программ осуществляется на уровнях: 1) аппаратуры; 2) программного обеспечения; 3) данных; 4) канальном; 5) сеансовом; 6) прикладном

+ 1, 2, 3
4, 5, 6
1, 3, 5
2, 4, 6

Из перечисленного контроль доступа используется на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом

+ 1, 2, 5
1, 2, 3
4, 5, 6
1, 3, 5

Из перечисленного метка безопасности состоит из таких компонентов, как 1) уровень секретности; 2) категория; 3) множество ролей; 4) ключ шифра; 5) области

+ 1, 2, 5
1, 2, 3
3, 4, 5
1, 3, 5

Из перечисленного методами защиты потока сообщений являются: 1) нумерация сообщений; 2) отметка времени; 3) использование случайных чисел; 4) нумерация блоков сообщений; 5) копирование потока сообщений

+ 1, 2, 3
3, 4, 5
1, 3, 5
2, 4

Из перечисленного на сетевом уровне рекомендуется применение услуг: 1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности; 6) аутентификации

+ 2, 4, 5, 6
1, 2, 3
4, 5, 6
2, 4, 6

Из перечисленного на транспортном уровне рекомендуется применение услуг: 1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности; 6) аутентификации

+ 2, 4, 5, 6
2, 4, 6
1, 2, 3
4, 5, 6

Из перечисленного объектами для монитора обращений являются: 1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты; 6) устройства

+ 2, 3, 4, 6
1, 2, 3, 4
1, 3, 5
2, 4, 6

Из перечисленного подсистема управления криптографическими ключами структурно состоит из: 1) центра распределения ключей; 2) программно-аппаратных средств; 3) подсистемы генерации ключей; 4) подсистемы защиты ключей

+ 1, 2
3, 4
1, 3
2, 4

Из перечисленного пользователи СУБД разбиваются на категории: 1) системный администратор; 2) сетевой администратор; 3) администратор сервера баз данных; 4) администратор базы данных; 5) конечные пользователи; 6) групповые пользователи

+ 3, 4, 5
1, 3, 6
1, 2, 5
4, 5, 6

Из перечисленного привилегии в СУБД могут передаваться: 1) субъектам; 2) группам; 3) ролям; 4) объектам; 5) процессам

+ 1, 2, 3
3, 4, 5
1, 3, 5
2, 4, 5

Из перечисленного привилегии СУБД подразделяются на категории: 1) чтения; 2) безопасности; 3) доступа; 4) тиражирования

+ 2, 3
1, 2
3, 4
1, 4

Из перечисленного привилегиями безопасности являются: 1) security; operator; 2) create trace; 3) createdb; 4) operator; 5) trace

+ 1, 3, 4, 5
1, 2, 3, 5
2, 4, 5
1, 2, 4

Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером

+ 2, 3, 4
1, 2, 3
3, 4, 5
1, 4, 5

Из перечисленного система защиты электронной почты должна: 1) обеспечивать все услуги безопасности; 2) обеспечивать аудит; 3) поддерживать работу только с лицензионным ПО; 4) поддерживать работу с почтовыми клиентами; 5) быть кросс-платформенной

+ 1, 4, 5
2, 3, 4
1, 2, 3
1, 3, 5

Из перечисленного составляющими информационной базы для монитора обращений являются: 1) виды доступа; 2) программы; 3) файлы; 4) задания; 5) порты; 6) форма допуска

+ 1, 6
2, 3
4, 5
2, 4

Из перечисленного субъектами для монитора обращений являются: 1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты; 6) устройства

+ 1, 2, 5
1, 2, 3
4, 5, 6
2, 3, 5

Из перечисленного типами услуг аутентификации являются: 1) идентификация; 2) достоверность происхождения данных; 3) достоверность объектов коммуникации; 4) причастность;

+ 2, 3
1, 4
1, 2
3, 4

Из перечисленного цифровая подпись используется для обеспечения услуг: 1) аутентификации; 2) целостности; 3) контроля доступа; 4) контроля трафика

+ 1, 2
3, 4
1, 3
2, 4

Из перечисленного электронная почта состоит из: 1) электронного ключа; 2) расширенного содержания письма; 3) краткого содержания письма; 4) тела письма; 5) прикрепленных файлов

+ 3, 4, 5
1, 2, 3
1, 4, 5
2, 3, 4

Из перечисленного ядро безопасности ОС выделяет типы полномочий: 1) ядра; 2) периферийных устройств; 3) подсистем; 4) пользователей

+ 1, 3
2, 3
1, 2
3, 4

Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются: 1) нормативы; 2) ограничения; 3) стандарты; 4) правила

+ 2, 4
1, 2
3, 4
1, 3

Из перечисленного: 1) администраторы; 2) пользователи; 3) задания; 4) терминалы; 5) программы; 6) файлы - модель политики безопасности Адепт-50 рассматривает следующие группы безопасности

+ 2, 3, 4, 6
1, 2, 3, 4
3, 4, 5, 6
1, 2, 5, 6

Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ потенциальных угроз - процесс анализа рисков при разработке системы защиты ИС включает

+ 3, 4
1, 2
1, 3
2, 4

Из перечисленного: 1) занижение уровня секретности; 2) завышение уровня секретности; 3) запись вслепую; 4) лишняя запись; 5) удаленная запись; 6) привилегированные субъекты - проблемами модели Белла-ЛаПадула являются

+ 2, 3, 5, 6
1, 2, 3, 4
4, 5, 6
2, 3, 4

Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности - согласно "Оранжевой книге" требованиями в области аудита являются

+ 1, 2
3, 4
1, 3
2, 4

Из перечисленных типов: 1) перехватчики; 2) имитаторы; 3) наблюдатели; 4) фильтры; 5) заместители - все клавиатурные шпионы делятся на

+ 2, 4, 5
1, 2, 3, 5
2, 3, 4
1, 3, 4

Из перечисленных требований: 1) резервное копирование; 2) аутентификация; 3) необходимость записи всех движений защищаемых данных; 4) накопление статистики - при разработке протоколирования в системе защиты учитываются

+ 3, 4
1, 2
2, 3
1, 4

Из перечисленных уровней безопасности: 1) базовый; 2) низкий; 3) средний; 4) стандартный; 5) высокий - в "Европейских критериях" определены

+ 1, 3, 5
1, 2, 5
2, 3, 4
2, 3, 5

Как предотвращение неавторизованного использования ресурсов определена услуга защиты

+ контроль доступа
целостность
аутентификация
причастность

Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем

+ сетевом
транспортном
физическом
канальном

Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

+ за определенное время
фиксированным ресурсом
ограниченной компетенцией злоумышленника
фиксированными затратами

На _____уровне ОС происходит определение допустимых для пользователя ресурсов ОС

+ системном
сетевом
внешнем
приложений

На многопользовательские системы с информацией одного уровня конфиденциальности согласно "Оранжевой книге" рассчитан класс

+ С1
В1

C2
B2

Надежность СЗИ определяется

+ самым слабым звеном
самым сильным звеном
усредненным показателем
количеством отраженных атак

Наименее затратный криптоанализ для криптоалгоритма DES

+ перебор по всему ключевому пространству
перебор по выборочному ключевому пространству
разложение числа на простые множители
разложение числа на сложные множители

Наименее затратный криптоанализ для криптоалгоритма RSA

+ разложение числа на простые множители
разложение числа на сложные множители
перебор по выборочному ключевому пространству
перебор по всему ключевому пространству

Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем

+ транспортном
канальном
сетевом
сеансовом

Обеспечение целостности информации в условиях случайного воздействия изучается

+ теорией помехоустойчивого кодирования
криптоанализом
стеганографией
криптологией

Обычно в СУБД применяется управление доступом

+ произвольное
декларируемое
административное
иерархическое

Операционная система Windows 2000 отличает каждого пользователя от других по

+ идентификатору безопасности
маркеру доступа
дескриптору защиты
маркеру безопасности

Операционная система Windows NT соответствует уровню Оранжевой книги:

+ C2
C3
C5
C4

Организационные требования к системе защиты

+ административные и процедурные
аппаратурные и физические
административные и аппаратурные
управленческие и идентификационные

Основной целью системы брандмауэра является управление доступом

+ к защищаемой сети
внутри защищаемой сети
к архивам
к секретной информации

Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему

+ хотя бы одного средства безопасности
всех средств безопасности
пароля
аудита

Таблица 6 – Критерии оценки сформированности компетенций

Код и наименование индикатора достижения компетенции (части компетенции)	Критерии оценивания сформированности компетенции (части компетенции)
	соответствует оценке «зачтено» 50-100% от максимального балла
ИД-1-$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2- $_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3- $_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4- $_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	владеет материалом по теме, но допускает неточности при формулировке основных понятий, в основном правильно анализирует задачу, выделяя ее базовые составляющие; достаточно эффективно осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи; планирует возможные варианты решения задачи, оценивая их достоинства и недостатки; достаточно полно определяет и оценивает последствия возможных решений задачи, определяет источники информации на основе поставленных целей для решения экономических задач; не вполне уверенно определяет методы сбора, обработки информации, способы и вид ее представления; разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов, может допускать неточности при проведении экономическую оценку мероприятий по воздействию на риск, что не оказывает существенного влияния на общий уровень сформированности компетенций.

1. ОПРЕДЕЛЕНИЕ РЕЗУЛЬТАТА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма промежуточной аттестации по дисциплине *экзамен*.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СРЕДСТВА ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Выберите один правильный вариант ответа:

1. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:

+Федеральная служба по техническому и экспортному контролю при Президенте РФ

Федеральная служба безопасности Российской Федерации

Служба внешней разведки Российской Федерации

2. Защита информации – это …

комплекс мероприятий, направленных на обеспечение информационной безопасности

совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

+все определения корректны

Дайте развернутый ответ на вопрос.

1. В чьем ведении находятся вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России? рассматривает:

Правильный ответ:

Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает Федеральная служба по техническому и экспортному контролю при Президенте РФ.

2. Понятие политики безопасности.

Правильный ответ:

Политика безопасности это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

3. Нарушения информационной безопасности, за которые не предусмотрена уголовная ответственность.

Правильный ответ:

Уголовный кодекс РФ не предусматривает наказания за +ведение личной корреспонденции на производственной технической базе; +нарушение правил эксплуатации информационных систем.

4. Понятие документированной информации.

Правильный ответ:

Документированной информацией называют информацию, зафиксированную на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

5. Содержание и структура законодательства в области информационной безопасности

Правильный ответ:

Содержание и структура законодательства в области информационной безопасности включает следующие нормативно-правовые акты: Конституция Российской Федерации, Указы Президента Российской Федерации, Подзаконные акты Правительства Российской Федерации, Федеральные законы, Кодексы.

6. Предмет правового регулирования в области информации, информационных технологий и защиты информации.

Правильный ответ:

Предметом правового регулирования в области информации, информационных технологий и защиты информации являются отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

7. Условия действительности электронной цифровой подписи.

Правильный ответ:

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; подтверждена подлинность электронной цифровой подписи в электронном документе; электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

8. Перечень видов деятельности в области зашиты информации, на которые необходима лицензия.

Правильный ответ:

К видам деятельности в области зашиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ – “О лицензировании отдельных видов деятельности” от 24.12.94 №1418, в частности, относится разработка, производство, реализация и сервисное обслуживание: шифровальных средств; защищенных систем телекоммуникаций; программных средств; специальных технических средств зашиты информации; подготовка и переподготовка кадров.

Пкос-5 Способен разрабатывать мероприятия по воздействию на риск в разрезе отдельных видов и проводить их эконом

Выберите один правильный вариант ответа:

2. Сертификации подлежат:

+средства криптографической защиты информации;

средства выявления закладных устройств и программных закладок;

защищенные технические средства обработки информации;

защищенные информационные системы и комплексы телекоммуникаций;

3. Что представляет собой Доктрина информационной безопасности РФ?

Нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;

федеральный закон, регулирующий правоотношения в области информационной безопасности;

целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

+совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Дайте развернутый ответ на вопрос.

1. Понятие идентификации.

Правильный ответ:

Идентификация это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации.

2. Понятие безопасности информации

Правильный ответ:

Безопасность информации это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.

3. Понятие электронной подписи

Правильный ответ:

Электронной подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

4. Управлением риском это –

Правильный ответ:

Управлением риском называется процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска.

5. Понятие программной закладки

Правильный ответ:

Программными закладками называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на информационные системы. Защита от программных закладок обеспечивается аппаратным модулем, устанавливаемым на системную шину ПК.

6. Классификация средств защиты информации.

Правильный ответ:

Согласно "Европейским критериям" безопасность может считаться высокой, средней и базовой. Высокая может быть преодолена только государственной спецслужбой, средняя способна противостоять корпоративному злоумышленнику, базовая способна противостоять отдельным атакам.

7. Понятие аутентификации.

Правильный ответ:

Аутентификация это проверка подлинности пользователя по предъявленному им идентификатору. Аутентификация используется на уровнях сетевом, транспортном и прикладном уровнях.

8. Понятие и классификация брандмауэра.

Правильный ответ:

Брандмауэром называется система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Брандмауэры первого поколения представляли маршрутизаторы с фильтрацией пакетов, брандмауэры второго поколения представляли собой "уполномоченные серверы", брандмауэры третьего поколения используют для фильтрации специальные многоуровневые методы анализа состояния пакетов.

Таблица 7 – Критерии оценки сформированности компетенций

Код и наименование индикатора достижения компетенции (части компетенции)	Критерии оценивания сформированности компетенции (части компетенции)
	соответствует оценке «зачтено» 50-100% от максимального балла
ИД-1-$_{УК-1}$ Анализирует задачу, выделяя ее базовые составляющие ИД-2- $_{УК-1}$ Осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи ИД-3- $_{УК-1}$ Планирует возможные варианты решения задачи, оценивая их достоинства и недостатки ИД-4- $_{УК-1}$ Определяет и оценивает последствия возможных решений задачи ИД-1-$_{ПКос-5}$ Разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов ИД-2-$_{ПКос-5}$ Проводит экономическую оценку мероприятий по воздействию на риск	владеет материалом по теме, но допускает неточности при формулировке основных понятий, в основном правильно анализирует задачу, выделяя ее базовые составляющие; достаточно эффективно осуществляет поиск и критический анализ информации, необходимой для решения поставленной задачи; планирует возможные варианты решения задачи, оценивая их достоинства и недостатки; достаточно полно определяет и оценивает последствия возможных решений задачи, определяет источники информации на основе поставленных целей для решения экономических задач; не вполне уверенно определяет методы сбора, обработки информации, способы и вид ее представления; разрабатывает мероприятия по воздействию на риск в разрезе отдельных видов, может допускать неточности при проведении экономическую оценку мероприятий по воздействию на риск, что не оказывает существенного влияния на общий уровень сформированности компетенций.

Дополнительные контрольные испытания

для студентов, набравших менее 50 баллов (в соответствии с Положением «О модульно-рейтинговой системе»), формируются из числа оценочных средств по темам, которые не освоены студентом.