МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»
в г. Белово

УТВЕРЖДАЮ

Заместитель директора
по учебной работе,
совмещающая должность
директора филиала
Долганова Ж.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Приложение к рабочей программе по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Квалификация выпускника: Специалист

Специальность 38.05.01 Экономическая безопасность

специализация «01 Экономико-правовое обеспечение экономической безопасности»

Формы обучения очно-заочная

Кафедра Инженерно-экономическая

Год набора 2023

Белово, 2024

Автор (составитель) ФОС по дисциплине: Информационная безопасность в профессиональной деятельности

ФИО, ученая степень, должность: ст. преподаватель Аксененко Е.Г.

кафедра Экономики и информационных технологий
(наименование кафедры)

Фонд оценочных средств по дисциплине обсужден на заседании кафедры экономики и информационных технологий
Протокол № 8 от 13.04.2024г.

Зав. экономики и информационных технологий

Согласовано учебно-методической комиссией

по специальности 38.05.01 Экономическая безопасность

Протокол № 8 от 13.04.2024г.

Председатель учебно-методической комиссии по специальности 38.05.01 Экономическая безопасность

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (ФОС) создается в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования для аттестации обучающихся на соответствие их учебных достижений поэтапным требованиям соответствующей ОПОП для проведения входного и текущего оценивания, а также промежуточной аттестации обучающихся. ФОС является составной частью нормативно-методического обеспечения системы оценки качества освоения ОПОП ВО, входит в состав ОПОП. ФОС – комплект методических материалов, нормирующих процедуры оценивания результатов обучения, т.е. установления соответствия учебных достижений запланированным результатам обучения и требованиям образовательных программ, программ учебных дисциплин (модулей).

ФОС сформирован на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности добиться успеха.

ФОС по дисциплине «Информационная безопасность в профессиональной деятельности» включает все виды оценочных средств, позволяющих проконтролировать освоение обучающимися компетенций, предусмотренных ФГОС ВО по специальности 38.05.01. «Экономическая безопасность» и программой учебной дисциплины «Основы информационных технологий».

ФОС предназначен для профессорско-преподавательского состава и обучающихся филиала КузГТУ в г.Белово. ФОС подлежит ежегодному пересмотру и обновлению.

2. ПАСПОРТ КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ

Профессиональные компетенции (ПК)

ПК-3 - Способность создавать системы управления финансово-экономическими показателями и мониторинга финансово-экономических показателей организации с применением информационных технологий, определять возможности использования готовых проектов, алгоритмов, пакетов прикладных программ.

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень

Опрос по контрольным вопросам, подготовка отчетов по лабораторным работам, тестирование	ПК-3	Выполняет создание систем управления финансовоэкономическими показателями и мониторинга финансовоэкономических показателей организации с применением информационных технологий, определять возможности использования готовых проектов, алгоритмов, пакетов прикладных программ	Знать: принципы, методы и средства создания систем управления финансово экономическими показателями и мониторинга финансово-экономических показателей организации с применением информационных технологий, определять возможности использования готовых проектов, алгоритмов, пакетов прикладных программ; Уметь: создавать системы управления финансово экономическими показателями и мониторинга финансово-экономических показателей организации с применением информационных технологий; определять возможности использования готовых проектов, алгоритмов, пакетов прикладных программ Владеть: навыками создания систем управления финансово-экономическими показателями и мониторинга финансово-экономических показателей организации с применением информационных технологий, определением возможности использования готовых проектов, алгоритмов, пакетов прикладных программ.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции -** компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции -** компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

3. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ

по дисциплине **Информационная безопасность в профессиональной деятельности**

3.1. Описание назначения и состава фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав образовательной программы и предназначен для текущего и промежуточного контроля и оценки планируемых результатов обучения – знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе прохождения подготовки по дисциплине **Основы информационных технологий**

ФОС разработан на основании:

– федерального государственного образовательного стандарта высшего образования по направлению подготовки _____38.05.01. «Экономическая безопасность» _____

– образовательной программы высшего образования по направлению подготовки _____Специалист 38.05.01. «Экономическая безопасность» _____

Направленность (профиль) «01 Экономико-правовое обеспечение экономической безопасности»

код и наименование направления подготовки, уровень подготовки

3.2. Перечень компетенций, формируемых в процессе прохождения дисциплины

ПК-3

3.3. Этапы формирования и оценивания компетенций

№ п/п	Контролируемые разделы (темы)	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
4 курс 8 семестр				
1.	Понятия информатика, информация, данные. Понятия авторизация, идентификация, аутентификация.	ПК-3	Лабораторная работа	
2	Персональные данные. Требования закона №152 «О персональных данных», ответственность за нарушения работы с персональными данными, классификация персональных данных, составление документов для разрешения работы с персональными данными.	ПК-3	Практическая работа	
3	Защита информации. Риски, связанные с информацией (конфиденциальность, целостности, доступность), методы уменьшения рисков, определение потенциальных и реальных угроз	ПК-3	Практическая работа	

4	Преступления в сфере компьютерных технологий. Статьи УК РФ, связанные с преступлениями в сфере компьютерных технологий, наказание, противодействие атакам злоумышленников.	ПК-3	Практическая работа	
5	Шифрование. Методы шифрования данных, аппаратные и программные средства шифрования данных, открытые/закрытие ключи, государственные стандарты в области шифрования данных, симметричное/ асимметричное шифрование, криптографические хешфункции	ПК-3	Практическая работа	
6	Электронно-цифровая подпись. Электронная цифровая подпись, виды электронно-цифровых подписей, хеш-функции в задачах прописывания документов	ПК-3	Практическая работа	Экзамен

4. ВХОДНОЙ КОНТРОЛЬ

4.1 Цель входного контроля – определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты, полученные при входном оценивании обучающегося, используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

4.2 Описание оценочных средств

Форма проведения входного контроля – бланковое тестирование. Количество вопросов – 20, длительность тестирования – 45 минут.

4.2.1 Шкала оценивания (методика оценки)

За каждый правильный ответ выставляется один балл.

Оценка формируется в соответствии с критериями таблицы:

Максимальный балл	Проходной балл	Оценка
20	не менее 18	отлично
17	не менее 15	хорошо
14	не менее 11	удовлетворительно
10	-	неудовлетворительно

4.2.2 Задания (вопросы) для входного контроля обучающихся.

Для освоения дисциплины необходимы компетенции (знания умения, навыки и (или) опыт деятельности, полученные в рамках изучения следующих дисциплин: «Основы информационных технологий» Вопросы входного контроля охватывают материалы данных дисциплин.

Перечень вопросов входного контроля

1. Понятие данных. Понятие информации
2. Свойства информации
3. Классификация информационной технологии
4. Что является толчком для стремительного развития информационных технологий?
5. Понятие информационной системы.
6. Что такое пакет прикладных программ
7. Какие программы входят в ППП?
8. Для чего предназначен текстовый редактор?
9. Виды документов, создаваемых с помощью текстового процессора Word
10. Для чего предназначен табличный редактор?
11. Понятия ячейка, строка, столбец в табличном редакторе
12. Типы данных, которые может содержать ячейка
13. Что означает относительная ссылка?
14. Что означает абсолютная ссылка?
15. Как включить формулу в текст документа?
16. Виды диаграмм в табличном редакторе.
17. Как вставить диаграмму?
18. С помощью какой программы создать презентацию?
19. Какие объекты можно вставить в презентацию?
20. Зачем используется анимация в презентациях?

5. Текущий контроль
по дисциплине И**нформационная безопасность в профессиональной деятельности**

5.1 Оцениваемые компетенции ПК-3
5.2 Форма контроля устный опрос при защите лабораторной, практической работы
5.3 Критерии и шкала оценивания
Шкала оценивания

Баллы	Степень удовлетворения критериям
5 баллов «Отлично»	Указание точных названий и определений, правильная формулировка понятий и категорий, приведены все необходимые формулы, проставлены все единицы измерения, есть соответствующая статистика и т.п., все задания выполнены верно (все задачи решены правильно).
4 балла «Хорошо»	Одна-две несущественные ошибки в определении понятий и категорий, в формулах, статистических данных и т. п., кардинально не меняющие суть изложения, наличие незначительного количества грамматических и стилистических ошибок, одна-две несущественные погрешности при выполнении заданий или в решениях задач.
3 балла «Удовлетворительно»	Ответ отражает лишь общее направление изложения лекционного материала, наличие более двух несущественных или одной-двух существенных ошибок в определении понятий и категорий, формулах, статистических данных и т. п.; большое количество грамматических и стилистических ошибок, одна-две существенные ошибки при выполнении заданий или в решениях задач.
2 балла «Неудовлетворительно»	Обучающийся демонстрирует слабое понимание программного материала. Тема не раскрыта, более двух существенных ошибок в определении понятий и категорий, в формулах, статистических данных, при выполнении заданий или в решениях задач, наличие грамматических и стилистических ошибок и др. Нет ответа. Не было попытки выполнить задание.

5.4 Материалы для устного опроса

Контрольные вопросы

Тема 1.
1. Информатика это -.
2. Информация это -
3. Данные это -
4. Понятие авторизация.
5. Понятие идентификация.
6. Понятие аутентификация.

Тема 2.
1. Что относится к персональным данным.
2. Закон о персональных данных.
3. Ответственность за нарушения персональных данных.
4. Классификация персональных данных.
5. Составление документов при работе с персональными данными.

Тема 3.
1. Понятие конфиденциальности.
2. Понятие целостности.
3. Понятие доступности.
4. Методы уменьшения рисков.
5. Определение потенциальных и реальных угроз.
Тема 4.
1. Преступления в сфере компьютерных технологий.
2. Статьи УК РФ, связанные с преступлениями в сфере компьютерных технологий.
3. Наказания за преступления в сфере компьютерных технологий
4. Противодействие атакам злоумышленников.
Тема 5..
1. Что понимается под шифрованием данных..
2. Методы шифрования данных.
3. Что такое открыты/закрытый ключ.
4. Симметричное/ассиметричное шифрование.
5. Криптографические кэшфункции.
Тема 6.
1. Для чего используется электронно-цифровая подпись
2. Виды электронно-цифровых подписей.
3. Хеш-функции в задачах прописывания документов.
4. Технология использования ЭЦП.
5. Плюсы и минусы ЭЦП.

Отчеты по лабораторным и (или) практическим работам:
По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате
Содержание отчета:
1. Тема работы.
2. Задачи работы.
3. Краткое описание хода выполнения работы.
4. Ответы на задания или полученные результаты по окончании выполнения работы
5. Выводы.

Критерии оценивания:
75 – 100 баллов – при раскрытии всех разделов в полном объеме
0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

6. КОНТРОЛЬ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ
по дисциплине И**нформационная безопасность в профессиональной деятельности**

6.1 **Оцениваемые компетенции** ПК-3

6.2 Самостоятельная работа заключается в изучении учебного материала по темам дисциплины. Оформление отчетов по лабораторным, практическим работам. Подготовка к практическим занятиям. Контроль самостоятельной работы осуществляется в процессе защиты практических, лабораторных работ при ответах

на контрольные вопросы, при проверке правильности и качества оформления отчетов. Подготовка к тестированию. Выполнение теста по окончании изучения темы.

7. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

по дисциплине **Информационная безопасность в профессиональной деятельности**

7.1 Оцениваемые компетенции ПК-3

7.2 Вид аттестации экзамен

Формой промежуточной аттестации является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций. Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты обучающихся по лабораторным и (или) практическим работам;
- ответы обучающихся на вопросы во время опроса.

На экзамене обучающийся отвечает на билет, в котором содержится 2 вопроса. Оценка за экзамен выставляется с учетом отчетов по лабораторным работам и ответа на вопросы.

7.3 Критерии и шкала оценивания

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:
85 –100 баллов – при правильном и полном ответе на два вопроса;
75 –84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
65 –74 баллов – при правильном и неполном ответе только на один из вопросов;
0–49 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-64	65-74	75-84	85-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к зачету:

1. Виды информации.
2. Отличие данных и информации.
3. Понятия идентификация, авторизация.
4. Особенности классов персональных данных.
5. Закон о персональных данных
6. Ответственность за нарушения персональных данных
7. Классификация персональных данных
8. Понятие целостности, доступности и конфиденциальности.
9. Риски, связанные с информацией.
10. Методы уменьшения рисков.
11. Определение потенциальных и реальных угроз.
12. Виды преступлений, связанных с компьютерными технологиями.
13. Наказания за преступления в сфере компьютерных технологий.
14. Противодействия атакам злоумышленников.
15. Виды шифрования, цель шифрования.
16. Определение открытого/закрытого ключа.
17. Симметричное/ассиметричное шифрование.
18. Цель электронно-цифровой подписи, виды ЭЦП.
19. Плюсы и минусы ЭЦП.

20. Технология использования ЭЦП.

Тестовая база

ПК-3 - Способность создавать системы управления финансово-экономическими показателями и мониторинга финансово-экономических показателей организации с применением информационных технологий, определять возможности использования готовых проектов, алгоритмов, пакетов прикладных программ

1	Соотнесите основные понятия в области информационной безопасности: 1. Атака 2. Уязвимость АС 3. Угроза безопасности АС 4. Защищенная система a. некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы b. система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности c. возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности d. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы **ОТВЕТ: 1-d; 2-a; 3-c; 4-b;**
2	Соотнесите основные виды угроз для АС: 1. Угроза нарушения конфиденциальности 2. Угроза отказа служб 3. Угроза нарушения целостности a. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую b. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС c. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней **ОТВЕТ: 1-c; 2-b; 3-a**
3	Соотнесите классификацию угроз по ряду признаков: 1. по природе возникновения 2. по непосредственному источнику 3. по степени воздействия на АС 4. по способу доступа к ресурсам АС a. пассивные и активные b. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС c. естественные или искусственные d. природная среда, человек, санкционированные программные средства и несанкционированные программные средства **ОТВЕТ: 1-b; 2-d; 3-c;4-a**
4	Соотнесите интересы в области информационной безопасности: 1. Национальные интересы

	2. Интересы личности 3. Интересы государства 4. Интересы общества a. состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина b. обеспечиваются институтами государствен ной власти, осуществляющими свои функции, в том числе во взаимодей ствии с действующими на основе Конституции РФ и законодательства РФ общественными организациями c. состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политиче ской, экономической и социальной стабильности, в безусловном обеспе чении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества. d. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании обще ственного согласия, в духовном обновлении России. **ОТВЕТ: 1-2; 2-1; 3-3; 4-4.**
5	Соотнесите основные методы получения паролей: 1. метод тотального перебора 2. словарная атака 3. получение паролей из самой системы на основе программной и аппаратной реализации конкретной системы 4. проверка паролей, устанавливаемых в системах по умолчанию a. для перебора используется словарь наиболее вероятных ключей b. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей c. опробываются все ключи последовательно, один за другим d. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе **ОТВЕТ: 1-c; 2-a; 3-b; 4-d;**
6	Соотнесите функции, выполняемые техническими средствами защиты: 1. внешняя защита 2. опознавание 3. внутренняя защита a. защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации b. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД c. специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам **ОТВЕТ: 1-b; 2-c; 3-a**
7	_____ — это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы. Ответ: Авторизация
8	_____ — это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации. Ответ: Идентификация

9	_____ — это проверка подлинности пользователя по предъявленному им идентификатору. Ответ: Аутентификация
10	_____ — это свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов. Ответ: Конфиденциальность
11	_____ — это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования. Ответ: Безопасность информации
12	_____ называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения. Ответ: Электронной подписью
13	Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство Ответ: Доступность
14	Восстановление данных является дополнительной функцией услуги защиты Ответ: Целостность
15	Два ключа используются в криптосистемах Ответ: С открытым ключом
16	Единственный ключ используется в криптосистемах Ответ: Симметричных
17	С помощью закрытого ключа информация: Ответ: Расшифровывается
18	С помощью открытого ключа информация: Ответ: Зашифровывается
19	Длина исходного ключа в ГОСТ 28147-89 (бит): Ответ: 256
20	Длина исходного ключа у алгоритма шифрования DES (бит): Ответ: 56
21	Механизм определения того, является ли пользователь тем, за кого себя выдает, называется: Ответ: аутентификацией
22	Виды информационной безопасности: 1. **Персональная, корпоративная, государственная** 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная
23	Основные объекты информационной безопасности: **1. Компьютерные сети, базы данных** 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы
24	Когда получен спам по e-mail с приложенным файлом, следует: 1. Прочитать приложение, если оно не содержит ничего ценного – удалить 2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама 3. **Удалить письмо с приложением, не раскрывая (не читая) его**
25	«Персональные данные» это: 1. **Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу**

	2. Фамилия, имя, отчество физического лица 3. Год, месяц, дата и место рождения, адрес физического лица 4. Адрес проживания физического лица 5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»
26	Наиболее важным при реализации защитных мер политики безопасности является: 1. Аудит, анализ затрат на проведение защитных мер 2. Аудит, анализ безопасности 3. **Аудит, анализ уязвимостей, риск-ситуаций**
27	Наиболее распространены угрозы информационной безопасности сети: 1. Распределенный доступ клиент, отказ оборудования 2. Моральный износ сети, инсайдерство 3. **Сбой (отказ) оборудования, нелегальное копирование данных**
28	Утечкой информации в системе называется ситуация, характеризуемая: 1. **Потерей данных в системе** 2. Изменением формы информации 3. Изменением содержания информации
29	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: 1. **Целостность** 2. Доступность 3. Актуальность 4. конфиденциальность
30	Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена 1. **конфиденциальность** 2. целостность 3. доступность 4. аутентичность
31	Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных: 1. Защита информации 2. **Компьютерная безопасность** 3. Защищенность информации 4. Безопасность данных
32	Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это: 1. государственная тайна 2. **коммерческая тайна** 3. банковская тайна 4. конфиденциальная информация
33	Исследование возможности расшифрования информации без знания ключей: 1. криптология 2. **криптоанализ** 3. взлом 4. несанкционированный доступ
34	Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это: 1. **Информационная безопасность** 2. Безопасность

	3. Национальная безопасность 4. Защита информации
35	Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами: 1. Служебная информация 2. Коммерческая тайна 3. Банковская тайна 4. **Конфиденциальная информация**
36	Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость: 1. Конфиденциальность 2. Целостность 3. **Доступность** 4. Аутентичность 5. Аппелируемость
37	Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ: 1. **Государственная тайна** 2. Коммерческая тайна 3. Банковская тайна 4. Конфиденциальная информация
38	К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…» 1. Информация без ограничения права доступа 2. **Информация с ограниченным доступом** 3. Информация, распространение которой наносит вред интересам общества 4. Объект интеллектуальной собственности 5. Иная общедоступная информация
39	Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте: 1. Государственная тайна 2. Коммерческая тайна 3. **Банковская тайна** 4. Конфиденциальная информация
40	Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п: 1. **черный пиар**; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.
41	Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей: 1. пиар; 2. **фишинг**; 3. нигерийские письма; 4. источник слухов; 5. пустые письма
42	Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

	1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож
43	Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным: 1. детектор; 2. доктор; 3. сканер; **4. ревизор;** 5. сторож.
44	Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние: 1. детектор; 2. **доктор**; 3. сканер; 4. ревизор; 5. сторож
45	Под непреднамеренным воздействием на защищаемую информацию понимают? 1. **Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений** 2. Процесс ее преобразования, при котором содержание информации изменяется на ложную 3. Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию 4. Не ограничения доступа в отдельные отрасли экономики или на конкретные производства
46	Шифрование информации это 1. **Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов** 2. Процесс преобразования, при котором информация удаляется 3. Процесс ее преобразования, при котором содержание информации изменяется на ложную 4. Процесс преобразования информации в машинный код
47	Как связаны ключи шифрования между собой? 1. **математической функцией** 2. связкой 3. шифром 4. специальным паролем
48	Свойством информации, наиболее актуальным при обеспечении информационной безопасности является: Ответ: Целостность
49	Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений? Ответ: тайна связи
50	ЭЦП –это… Ответ: электронно-цифровая подпись