

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
БУРЯТИЯ**

Государственное бюджетное профессиональное образовательное учреждение
**«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНФОРМАЦИОННО –
ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»**
(ГБПОУ «БРИЭТ»)

УТВЕРЖДАЮ
Замдиректора
_____ А.Б.Аюшиева
Приказ № _____
от « ____ » _____ 2023

**КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА/МОДУЛЯ)**

**ПМ 01 Участие в планировании и организации работ по
обеспечению защиты объекта**

**МДК 01.03 Организация работы персонала с
конфиденциальной информацией**

10.02.01 «Организация и технология защиты информации»

Срок освоения СПО по ППССЗ - 3 года 10 месяцев

Форма обучения – очная

Уровень образования при приеме на обучение – основное общее образование

Квалификация - техник по защите информации

г. Улан-Удэ
2023

Комплект оценочных средств учебной дисциплины/предмета/модуля разработан на основе требований Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО), утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 года № 805 с учетом получаемой специальности 10.02.01 Организация и технология защиты информации

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение «Бурятский республиканский информационно-экономический техникум»

Разработчик: _Парамонова Елена Георгиевна, преподаватель, 1 квал. категория

Комплект контрольно-оценочных средств рассмотрен на заседании ЦК ИТ

Протокол №_ от «__» _____ 2023 г.

Председатель ЦК _____ С.С.Бальчугова

Рецензент* _____

* Создаваемые комплекты КОС по ПМ должны проходить внешнюю экспертизу. Итоги экспертизы оформляются экспертным заключением или рецензией

СОДЕРЖАНИЕ

1. Паспорт фонда оценочных средств
2. Приложения
 - 2.1 Комплект тестов
 - 2.2 Перечень лабораторных работ и практических занятий
 - 2.4 Вопросы для устного (письменного опроса)
 - 2.5 Перечень самостоятельных работ

**Паспорт
фонда оценочных средств
по МДК 01.03 Организация работы персонала с конфиденциальной информацией**

Фонд оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом учебной дисциплины.

В результате освоения учебной дисциплины обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями:

-организовывать охрану персонала, территорий, зданий, помещений и продукции организаций (У1);

-пользоваться аппаратурой систем контроля доступа (У2);

-выделять зоны доступа по типу и степени конфиденциальности работ (У3);

-определять порядок организации и проведения рабочих совещаний (У4);

-использовать методы защиты информации в рекламой и выставочной деятельности (У5);

-использовать критерии подбора и расстановки сотрудников подразделений защиты информации (У6);

-организовывать работу с персоналом, имеющим доступ к конфиденциальной информации (У7);

-проводить инструктаж персонала по организации работы с конфиденциальной информацией (У8);

-контролировать соблюдение персоналом требований режима защиты информации (У9);

знать:

-виды и способы охраны объекта (З1);

-особенности охраны персонала организации (З2);

-основные направления и методы организации режима и охраны объекта (З3);

-разрешительную систему доступа к конфиденциальной информации (З4);

-принципы действия аппаратуры систем контроля доступа (З5);

-принципы построения и функционирования биометрических систем безопасности (З6);

-требования и особенности оборудования режимных помещений (З7);

-требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров (З8);

-требования режима защиты информации при приеме в организации посетителей (З9);

-организацию работы при осуществлении международного сотрудничества (З10);

-требования режима защиты информации в процессе рекламной деятельности (З11);

-требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати (З12);

-порядок оформления допуска лиц к конфиденциальным сведениям (З15);

-методы проверки персонала по защите информации (З16)

-процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией (З17).

Формой аттестации по учебной дисциплине является **комплексный экзамен** по ПМ 01. Концепция обеспечения безопасности информации в системе организации.

| № | Контролируемые умения, знания | Контролируемые разделы (темы) учебной дисциплины | Наименование оценочного средства |
|----|-------------------------------|---|---|
| 1 | | МДК 01.03 Организация работы персонала с конфиденциальной информацией. | |
| 2 | | Введение | |
| 3 | У7, У8, 31, 32 | Тема 1. Особенности работы с конфиденциальной информацией | СРС 1, подготовка к ПЗ, ПЗ 1 |
| 4 | У2, 35 | Тема 2. Документирование конфиденциальной информации. | СРС 1, ПЗ 2, 3, 4 |
| 5 | У 9, 316 | Тема 3. Организация конфиденциального документооборота | СРС 1, подготовка к ПЗ, ПЗ 5, 6 |
| 6 | У4, У7, У8, 37, 38, 39, 317 | Тема 4. Особенности работы с персоналом, владеющим конфиденциальной информацией | СРС 2, подготовка к ПЗ, ПЗ 7, 8, 9 |
| 7 | У3, 38, 310, 311, 312 | Тема 5. Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности | СРС2, СРС3, подготовка к ПЗ, ПЗ 10, 11 |
| 8 | У 1, 31, 33, 37,311, 312 | Тема 6. Подготовка конфиденциальных документов к архивному хранению и уничтожению. | СРС 1, СРС 3, подготовка к ПЗ, ПЗ 9 ПЗ 10 |
| 9 | У8, У9, 316, 317 | Тема 7. Режим конфиденциальности документированной информации. Особенности оборудования режимных помещений. | СРС3, подготовка к ПЗ, |
| 10 | | ДИФФЕРЕНЦИАЛЬНЫЙ ЗАЧЕТ | Т1 |

Условные обозначения: ЛР – лабораторная работа, ПЗ – практическое занятие, СР – самостоятельная работа, УО – устный ответ, Т – тестирование

КОМПЛЕКТ ТЕСТОВ

Учебная дисциплина МДК 01.03 Организация работы персонал с конфиденциальной информацией

Специальность 090905 Организация и технология защиты информации

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

| Темы | Номера тестовых заданий |
|--|-------------------------|
| Тема 1. Особенности работы с конфиденциальной информацией | 1,3 |
| Тема 2. Документирование конфиденциальной информации | 2 |
| Тема 3. Организация конфиденциального документооборота | 10 |
| Тема 4. Особенности работы с персоналом, владеющим конфиденциальной информацией | 4,13,14,19 |
| Тема 5. Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности | 7,8 |
| Тема 6. Подготовка конфиденциальных документов к архивному хранению и уничтожению. | 17,18 |
| Тема 7. Режим конфиденциальности документированной информации. Особенности оборудования режимных помещений. | 20 |

Критерии оценки

| Количество правильных ответов | Процент выполнения | Оценка |
|-------------------------------|--------------------|---------------------|
| | более 90% | Отлично |
| | 75-90% | Хорошо |
| | 50-74% | Удовлетворительно |
| | менее 50% | Неудовлетворительно |

ТЕСТОВЫЕ ЗАДАНИЯ

| № п/п вопроса | Содержание тестового задания | Варианты ответов |
|---------------|---|---|
| 1 | 2 | 3 |
| 1 | Обладатель информации – это... | а. обязательное для выполнения лицом, получившим доступ к определенной информации; б. <i>лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации;</i> в. это государственный служащий, который занимает государственную должность, связанную с непосредственным осуществлением задач и функций государственных органов. |
| 2 | Установите соответствие: 1. Конфиденциальность ПД; (б) 2. Документирование информации; (а) 3. Коммерческая тайна (в) | а. одно из обязательных условий включения информации и документов в информационные ресурсы любой организации; б. обязательное для соблюдения оператором или иным получившим доступ к ним лицом требование не допускать их распространения без согласия физ. лица или наличия иного законного основания; в. документированная информация ограниченного доступа, составляющая секрет производства (ноу- хау) |

| | | |
|----|--|---|
| 3 | Аббревиатура ДСП означает: | а. дисциплинарное судебное присутствие; б. договор строительного подряда; в. для служебного пользования. |
| 4 | Текущая работа с персоналом, обладающим КИ, включает в себя: | а. обучение и систематическое инструктирование сотрудников; б. проведение регулярной воспитательной работы; в. постоянный контроль за выполнением персоналом требований по защите КИ; г. проведение служебных расследований по факту утечки информации; д. возможны все варианты. |
| 5 | Установите соответствие: 1. 152-ФЗ (в) 2. 149-ФЗ (б) 3. 98-ФЗ (а) | а. "О коммерческой тайне" б. "Об информации, информационных технологиях и о защите информации" в. "О персональных данных" |
| 6 | Что из перечисленного не является целью проведения анализа рисков | а. делегирование полномочий б. количественная оценка воздействия потенциальных угроз в. выявление рисков г. определение баланса между воздействием риска и стоимостью необходимых контрмер |
| 7 | Безопасность информации – это | А) Совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также ее доступности для пользователей Б) Такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права; В) Такое ее состояние, при котором исключается возможность ее утечки за счет ПЭМИ и наводок, специальных устройств перехвата при передаче между объектами вычислительной техники Г) А и Б Д) Б и В |
| 8 | Эффективная программа безопасности требует сбалансированного применения: | А. Технические и нетехнические методов В. Контрмер и защитных механизмов С. Физической безопасности и технических средств защиты D. Процедур безопасности и шифрования |
| 9 | Тактическое планирование – это: | А. Среднесрочное планирование В. Долгосрочное планирование С. Ежедневное планирование D. Планирование на 6 месяцев |
| 10 | Вставьте пропущенное слово: «Криптографический элемент системы защиты информации - комплекс способов и средств защиты конфиденциальной информации методами _____». | А) Передачи данных. Б) Криптографии. В) Утечки информации из информационной системы. |
| 11 | Служебное расследование проводится в кратчайшие сроки в ходе служебного расследования анализируются следующие виды документов: | А) Письменное объяснение опрашиваемых лиц Б) Акты проверки документации и помещений. В) Другие документы относящиеся к расследованию (планы справки анонимные письма) Г. Все варианты |
| 12 | Если злоумышленник не ограничен в выборе объекта несанкционированного доступа, то эффективное противодействие его возможностям: | А) Требуется создания системы выявления угроз, которая функционировала бы непрерывно во времени. Б) Требуется создания системы выявления, предотвращения, отражения и локализации угроз, которая при необходимости могла бы использовать все законные средства, способы и методы. В) Требуется создания непрерывной эшелонированной, комплексной системы выявления, |

Перечень практических занятий:

- ПЗ 1. Обработка персональных данных без использования средств автоматизации.
- ПЗ 2. Разработка перечня конфиденциальной документированной информации.
- ПЗ 3. Определение степени ограничения доступа к документам.
- ПЗ 4. Использование отметки конфиденциальности при оформлении документов.
- ПЗ 5. Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация.
- ПЗ 6. Учет и регистрация внутренних конфиденциальных документов.
- ПЗ 7. Доступ к информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства.
- ПЗ 8. Доступ к информации, составляющей персональные данные
- ПЗ 9. Доступ к информации при ее предоставлении уполномоченным органам государственной власти.
- ПЗ 10. Учет конфиденциальной информации формирование конфиденциальных дел.
- ПЗ 11. Формирование конфиденциальных дел.
- ПЗ 12. Экспертиза ценности конфиденциальных документов.
- ПЗ 13. Подготовка конфиденциальных документов дел для архивного хранения и уничтожения.
- ПЗ 14. Обмен конфиденциальной документированной информацией.
- ПЗ 15. Проверка наличия носителей конфиденциальной информации.

Выполнение заданий к лабораторным работам и практическим занятиям, ответы на контрольные вопросы к ним способствуют контролю **умений** студентов по дисциплине.

Цели, задачи, задания, порядок проведения, контрольные вопросы, а также критерии оценки лабораторных работ и практических занятий представлены в методических указаниях к выполнению ПЗ по дисциплине.

Перечень вопросов для устного опроса

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

| Темы | Номера вопросов |
|--|-----------------|
| Тема.3.1 Организация офисной деятельности | 1, 2 |
| Тема 3.2. Основные направления обеспечения безопасности информационных ресурсов | 3,5,7 |
| Тема 3.3 Аналитическая работа в сфере безопасности информационных ресурсов | 4 |
| Тема 3.4. Особенности работы с персоналом, владеющим конфиденциальной информацией | 8-17 |
| Тема 3.5. Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности | 18-20 |
| Тема 3.6 Особенности оборудования режимных помещений | 21-23 |
| ЗАЧЕТ | |
| Тема 3.7. Право работника на защиту персональных данных | 24-27 |
| Тема 3.8. Обработка ПД работников | 28-30 |
| Тема 3.9. Защита конфиденциальной информации на предприятии | 31-32 |
| Тема 3.10. Организация защиты конфиденциальных сведений | 33-42 |
| Тема 3.11. Технология защиты конфиденциальных сведений | 43 |
| Тема 3.12. Законодательство в области защиты конфиденциальной информации | 44-45 |

ПЕРЕЧЕНЬ ВОПРОСОВ К ДИФ. ЗАЧЕТУ

- 1 Какие бывают каналы утраты информации
- 2 Что такое информационная безопасность предпринимательской деятельности
- 3 Какие этапы и методы аналитической работы вы знаете
- 4 Как получить доступ персонала к конфиденциальным сведениям, документам и базам данных
- 5 Что включают в себя конфиденциальные документы
- 6 Составьте технологическую цепочку приема сотрудников, работа которых связана с владением КИ
- 7 По какой причине от персонала информация легко переходит к злоумышленнику
- 8 На какие группы ошибочные и безответственные действия персонала подразделяются
- 9 Перечислите принципы построения разрешительной системы доступа
- 10 Что такое доступ
- 11 Какие задачи решаются при формировании здорового психологического климата
- 12 Перечислите основные формы контроля качества работы персонала
- 13 Что такое служебное расследование
- 14 Как происходит служебное расследование
- 15 Перечислите технологическую цепочку увольнения сотрудников
- 16 Что не разрешается участникам конфиденциального совещания
- 17 К посетителям - сотрудникам фирмы относятся
- 18 Что такое информационные документы
- 19 Что такое режим и охрана
- 20 Задачи режима и охраны

- 21 Имеет ли право работодатель устанавливать камеры наружного наблюдения в организации без согласия своих сотрудников
- 22 Что такое персональные документы
- 23 Организационные меры по защите персональных данных включают в себя
- 24 Кто такой оператор персональных данных
- 25 Назовите закон о персональных данных
- 26 Что такое обработка персональных данных работника
- 27 Назовите ФЗ о персональных данных
- 28 Что включает в себя письменное согласие субъекта на обработку ПД работника
- 29 Перечислите каналы распространения и утечки конфиденциальной информации
- 30 Что обязан работник в целях обеспечения достоверности ПД
- 31 Перечислите перечень локальных актов
- 32 Что такое разрабатываемый акт
- 33 Какие должны быть требования нормативно- правового акта
- 34 Какая ответственность предусмотрена за разглашение информации, составляющая коммерческую тайну
- 35 Кто обрабатывает персональные данные сотрудников
- 36 Кто может быть ответственным за организацию работы с ПД работников
- 37 Какие проводят мероприятия при подборе персонала для работы с конфиденциальной информацией
- 38 Что включает в себя обобщенные источники ценных сведений в процессе выставочной деятельности
- 39 Что следует сделать, что бы предотвратить разглашение ценных сведений в рекламно - выставочных материалах
- 40 Сотрудники, участвующие в мероприятиях по приему иностранных представителей обязаны
- 41 Особенности учета конфиденциальных документов и порядок их рассмотрения
- 42 Перечислите концепции национальной безопасности РФ
- 43 Перечислите уровни безопасности информации в организации

Перечень самостоятельных работ:

Самостоятельная работа:

1. Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).
2. Подготовка к практическим занятиям, оформление практических занятий, отчетов и подготовка к их защите.
3. Подготовка презентаций и рефератов по темам:
 - Безопасность деловой поездки
 - Требования к работникам
 - Организация физической охраны предприятия;
 - Персонал как основная опасность утраты конфиденциальной информации
 - Каналы утраты информации
 - Основные виды конфиденциальной информации, принятые в законодательстве РФ.
 - Особенности блокирования, прекращения обработки и уничтожения персональных данных работника
4. Изучение нормативных документов
5. Поиск дополнительной информации.
 - Оформление пакета документов, связанных с электронным документооборотом.
6. Подготовка к зачету
7. Подготовка к экзамену

В методических рекомендациях по выполнению самостоятельной работы студентов указаны цели, количество отведенного на них времени, содержание работы и критерии оценки.

ВОПРОСЫ К ЭКЗАМЕНУ

по учебной дисциплине МДК 01.03 Организация работы персонала с конфиденциальной информацией

специальность 10.02.01 Организация и технология защиты информации

1. Что запрещается относить к информации ограниченного доступа
2. Понятие «конфиденциальные документа». Что включают в себя конфиденциальные документы
3. Перечислите угрозы конфиденциальной информации
4. Понятие информационно - аналитической работы, функции ИАС
5. Этапы и методы аналитической работы
6. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией
7. Доступ персонала к конфиденциальным сведениям, документам и базам данных
8. Принципы построения разрешительной системы доступа
9. Особенности увольнения сотрудников, владеющих конфиденциальной информацией
10. Посягательства на собственность фирмы
11. Требования к помещениям, где происходит работа с конфиденциальными сведениями
12. Защищенный документооборот
13. Учет поступивших документов
14. Распределение, рассмотрение и направление документов на исполнение
15. Этапы подготовки конфиденциальных документов
16. Защита информации при работе с посетителем
17. Защита информации в работе кадровой службы
18. Нормативно- методические документы по обеспечению безопасности информации
19. Основы организации защиты против посягательств на собственность фирмы
20. Конфиденциальность, как главное условие защиты информации
21. Каналы утраты информации
22. Биометрические системы безопасности
23. Виды и способы охраны объекта
24. Понятие обработки персональных данных работника
25. Ответственность за разглашение сведений составляющих персональные данные
26. Организация защиты конфиденциальных сведений при приеме иностранных партнеров
27. Методы защиты информации в рекламной и выставочной деятельности
28. Процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией
29. Защита от утечки конфиденциальной информации
30. Концепции национальной безопасности РФ
31. Обеспечение безопасности внешней деятельности фирмы
32. Этапы снятия документов с контроля
33. Защита ПД при неавтоматизированной обработке.
34. Лицензирование деятельности организаций, связанных с конфиденциальной информацией
35. Персонал как основная опасность утраты конфиденциальной информации

36. Какие документы вправе потребовать при трудоустройстве, а какие нет
37. Особенности учета конфиденциальных документов и порядок их рассмотрения
38. Перечислите виды тайн и приведите примеры
39. Требования режима защиты информации в процессе рекламной деятельности
40. Организация внутриобъектового режима
41. Ответственность заместителя руководителя предприятия по безопасности в области защиты информации
42. Управленческие функции
43. Организация пропускного режима
44. Нормативно-методическая документация, регулирующая конфиденциальное делопроизводство.
45. Перечислите требования, предъявляемые к сотрудникам службы защиты информации.
46. Порядок уничтожения документов, дел и носителей информации
47. Методы добывания ценной информации
48. Каналы несанкционированного доступа