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 01.02 Организация работ подразделений защиты информации

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

Паспорт
комплекта оценочных средств
по междисциплинарному курсу МДК 01.02. Организация работ подразделений защиты информации

Комплект оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом междисциплинарного курса.

В результате освоения междисциплинарного курса обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями:

уметь:

- 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)

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)

Формой аттестации по учебной дисциплине является **зачет**

№	Контролируемые умения, знания	Контролируемые разделы (темы) учебной дисциплины	Наименование оценочного средства
1		**Тема 2.4. Организационные основы и принципы деятельности подразделений защиты информации**	**ТЕСТЫ**
2		Порядок создания подразделений защиты информации. Структура и содержание положения о подразделениях защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность подразделений защиты информации.	
3	У1, З1	Структура и содержание положения о подразделениях защиты информации. Состав и содержание других нормативных документов, регламентирующих	УО

		деятельность подразделений защиты информации.	
4	У1, З1	Основные принципы организации и деятельности подразделений защиты информации.	
5		Условия и факторы, влияющие на организацию работы подразделений защиты информации.	УО
6	З1, У2	Порядок взаимодействия подразделений защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.	
7	З2, У2	**Практическое занятие № 11** Организация взаимодействия службы защиты информации и подразделений предприятия	СР.1.1, ПЗ 11
8		**Тема 2.5. Подбор, расстановка и обучение сотрудников подразделений защиты информации**	ТЕСТЫ
9	З1, У2	Общие требования, предъявляемые к сотрудникам подразделений защиты информации. Особенности подбора кадров.	СР.1.2
10	У2, З1	Формы создания и способы поддержания необходимого микроклимата в коллективе.	УО
11	З2, У2	Формы повышения квалификации сотрудников.	
12	У1, З1	**Практическое занятие № 12** Методы получения информации о кандидатурах на должности.	СР.1.1, ПЗ12
13	У1, З1	**Практическое занятие № 13** Социально-психологические факторы, влияющие на расстановку кадров.	СР.1.1, ПЗ13
14		**Тема 2.6. Организация труда сотрудников подразделений защиты информации**	ТЕСТЫ
15	У1, З1	Деятельность сотрудников подразделений защиты информации. Обеспечение персональной ответственности за сохранность носителей информации.	
16	З3	Структура и содержание должностных инструкций сотрудников подразделений защиты информации.	УО
17	У1, З1	Организация рабочих мест сотрудников подразделений зашиты информации (рациональное размещение, оснащение оборудованием, техническими средствами).	
18	У1, З1	Обеспечение необходимых условий труда. Охрана труда.	
19	У2, З3	Карты организации трудового процесса.	
20	З3	**Практическое занятие № 14** Специфика деятельности сотрудников службы защиты информации.	СР.1.1, ПЗ14
21	З1, З2, З3	**Практическое занятие № 15** Социально-психологические факторы, влияющие на расстановку кадров	СР.1.1, ПЗ15

22	У1, З1	Распределение обязанностей между сотрудниками подразделений защиты информации.	
23		**Тема 2.7. Принципы и методы управления подразделений защиты информации**	ТЕСТЫ
24	У1, З1	Принципы управления подразделениями защиты информации.	УО
25	У1, З1	Понятие и сущность.	
26	У2, З3	Система методов управления.	
27	З3	Административно- методов управления правовые методы управления.	УО
28	З1, З2, З3	Экономические методы управления.	
29	З3	Социально-психологические методы управления.	УО
30	У1, З1	Взаимосвязь методов управления.	
31	У1, З1	Необходимость комплексного и системного применения методов управления службой защиты информации.	
32		**Тема 2.8. Технология управления подразделениями защиты информации**	ТЕСТЫ
33	З3	Состав управленческих функций. Содержание управленческих функций.	УО
34	З3	Технология управления подразделениями защиты информации.	СР.1.3
35	У1, З1	Значение управленческих решений	СР.1.3
36	У1, З1	Цели планирования. Виды планирования, их назначение.	УО
37	У2, З3	Содержание и структура планов.	СР.1.4
38	З3	Технология планирования.	УО
39	З3,	Методы и формы контроля выполнения планов	СР.1.5
40	У1, З1	Критерии эффективности подразделений защиты информации.	УО
41	З3	Методы оценки качества подразделений защиты информации	
42	У1, З1	Пути повышения эффективности управления подразделениями защиты информации.	УО
43	У1, З1	Способы повышения эффективности управления подразделением защиты информации.	
44	У2, З3	Зачет	

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

Приложение 1

КОМПЛЕКТ ТЕСТОВ

МДК 01.02.

Специальность 10.02.01 Организация и технология защиты информации

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

Темы	Номера тестовых заданий
Тема 2.4. Организационные основы и принципы деятельности подразделений защиты информации	1,2,3,4,5,6,7
Тема 2.5. Подбор, расстановка и обучение сотрудников подразделений защиты информации	8,9,10,11,12
Тема 2.6. Организация труда сотрудников подразделений защиты информации	13,14,15,16,17,18
Тема 2.7. Принципы и методы управления подразделений защиты информации	19,20,21,22,23,24
Тема 2.8. Технология управления подразделениями защиты информации	25,26,27,28

Критерии оценки:

Количество правильных ответов	Процент выполнения	Оценка
26-28	более 90%	Отлично
24-25	80-90%	Хорошо
20-23	60-79%	Удовлетворительно
Д0 18	менее 60%	Неудовлетворительно

ТЕСТОВЫЕ ЗАДАНИЯ

Тестовое задание	Вариант ответа
1. Сотрудники группы режима (функции):	А) наблюдение за обстановкой вокруг объекта и на его территории; Б)определяют перечень сведений, составляющих коммерческую тайну, если таковые сведения не упомянуты в общегосударственных документах; **В) разрабатывают положения и инструкции о порядке работы с конфиденциальной информацией и сведениями, составляющими тайну;** **Г) организуют и ведут закрытое делопроизводство, учет пользования, хранение и размножение документов и других, носителей конфиденциальной информации;**
2.Сотрудники группы охраны и сопровождения участвуют в:	**А) в организации прохода персонала и посетителей в различные зоны безопасности;**

	Б) в наблюдении за обстановкой вокруг объекта и на его территории; В) в экстренных действиях при возникновении угроз чрезвычайных обстоятельств; Г) осуществляют допуск персонала объекта к работе с конфиденциальной информацией, разрабатывают и осуществляют проверки выполнения сотрудниками объекта регламента работы с такой информацией;
3. В минимальный штатный состав СБ входят:	**А) Директор** **Б) Аналитик** В) Оперативный дежурный Г) Начальник отдела кадров **Д) Юрист** Е) Сотрудник делопроизводства **Ж) Сотрудник безопасности**
4. Целями обеспечения безопасности предприятия является:	**А)защита законных прав предприятия во взаимоотношениях с государственными органами, российскими и зарубежными партнерами и конкурентами; поддержание устойчивости порядка управления предприятием;** **Б)сохранение собственности предприятия, ее рационального и эффективного использования в направлении удовлетворения общественных потребностей;** В) предотвращение утечки, хищения, утраты, искажения, подделки информации; Г)повышение конкурентоспособности производимых товаров и услуг, создание благоприятной рыночной конъюнктуры для их реализации в условиях конкуренции на внутреннем и мировом рынке; рост прибылей предприятия; **Д)достижение внутренней и внешней организационной стабильности деятельности предприятия, надежности кооперированных связей и недопущение односторонней зависимости от случайных и недобросовестных партнеров;** Е) предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности
5. Операционная система Windows является :	**А) многозадачной** Б) однозадачной **В) многопользовательской** Г) однопользовательской
6. Атаки на ОС бывают:	**А) Локальными** Б) Глобальными **В) Удаленными** Г) Близкими
7. Профессиональный взлом имеет следующую структуру (восстановите последовательность)	А) попытка внедрения вредоносных программ

	Б) поиск уязвимостей в ПО ЗИ В) тщательный анализ ПО Г) анализ выбранной политики безопасности **Ответ Г,В,Б,А**
8. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:	**А) парольная аутентификация** Б) аутентификация по магнитному носителю В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
9. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:	А) парольная аутентификация **Б) аутентификация по магнитному носителю** В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
10. К защите от удаленного НСД можно отнести:	**А) модель рукопожатия** **Б) Протокол Kerberos** В) Аутентификация по биометрическим характеристикам Г) Аутентификация по росписи мышью
11. Целью защиты информации является:	А) предотвращение хищения, утечки, искажения, утраты и подделки информации; **Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;** В) реализация права на государственную тайну и конфиденциальную информацию Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации
12. К основным видам средств защиты информации относится:	**А) нормативно-правовые** **Б) Технические** В) Экологические Г) Этнические
13. Технические средства защиты – это	А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации **Б) это комплексы специального технического и программного обеспечения** В) правила и нормы поведения, направленные на обеспечение безопасности информации Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе
14. К каналам утечки информации относится:	**А) Магнитный канал** **Б) Виброакустический канал** **В) Лазерный канал** Г) Специальный канал
15. К назначению ОС относится:	А)управление процессором путем чередования выполнения программ; Б)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;

	В)управление памятью путем выделения программам на время их выполнения требуемой памяти; **Г)поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;**
16. Многопроцессорная обработка в ОС бывает:	**А) Симметричной** Б) Квадратичной В) Полной **Г) Ассиметричной**
17. К локальной защите от НСД относится:	**А) Аутентификация на основе биометрических характеристик** Б) Протокол CHAP **В) Парольная аутентификация** Г) Проток PAP
18. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:	А) парольная аутентификация Б) аутентификация по магнитному носителю В) модель рукопожатия **Г) аутентификация по характеристикам работы пользователя**
19. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.	А) PAP Б) CHAP **В) S/KEY** Г) Kerberos
20. К недостаткам дискреционного управления доступом относится:	**А) нельзя контролировать утечку конфиденциальной информации** Б) неудобство для пользователя В) нет опасности утечки конфиденциальной информации Г) слабая защита от вредоносных программ
21. В качестве основных задач системы безопасности рассматриваются:	А) своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушению его нормального функционирования и развития; **Б) создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;** **В) пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;** Г) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.
22. Сохранение коммерческой тайны, борьба с хакерами – это	А)Физическая безопасность **Б) Информационная безопасность** В) Экологическая безопасность Г) Экономическая безопасность

23. В соответствии с Федеральным законом от 8.08.2001 года №128–ФЗ деятельность различных подразделений службы безопасности предприятия подпадает под требования:	А) Заключать договор о неразглашении государственной тайны Б) Разрабатывать спецсредства для негласного получения информации **В) Лицензировать свои виды деятельности** Г) Предоставлять услуги в области шифрования
24. Анализ и прогноз динамики внешней и внутренней ситуации на предприятии, определение целей организационных структур службы безопасности, выявление проблем на пути достижения основной цели – это	А) Кадровое проектирование Б) Календарное управление В) Руководство **Г) Стратегическое управление**
25. Сотрудники этой группы участвуют в обеспечении безопасности деятельности объекта с помощью технических средств защиты	А) Детективная группа Б) Группа сопровождения **В) Техническая группа** Г) Группа безопасности
26. При организационном проектировании деятельности СБ предприятия первым этапом является:	А) Проектирование управленческой деятельности Б) Формулирование целей и задач системы управления **В) Анализ и прогноз внешней ситуации** Г) Расчет экономической эффективности Д) Решение основных вопросов формирования
27. Эта специализированная группа разрабатывает и проводит специальные мероприятия по изучению отдельных лиц из числа персонала объекта, посетителей и клиентов фирмы и жителей ближайшего к объекту окружения, в действиях которых содержатся угрозы безопасности деятельности объекта.	А) Группа сектора охранной безопасности Б) Специализированная группа подбора **В) Детективная группа** Г) Группа внешних расследования
28. Техническая группа	**А) Работает совместно с группой охраны** **Б) Отвечает за бесперебойную работу всех технических средств системы защиты объекта, ремонтирует и настраивает аппаратуру защиты** В) проверяют кандидатов для приема на работу на объекте; Г) по отдельным заданиям руководства разрабатывают и проводят специальные мероприятия в отношении фирм-конкурентов;

Рассмотрены на заседании ЦК ИТ

Протокол № ____ от «____» _____ 20__ г.

Председатель ЦК _____ С.С.Бальчугова

Приложение 2

Перечень практических занятий:

ПЗ11. Организация взаимодействия службы защиты информации и подразделений предприятия
ПЗ12 Методы получения информации о кандидатурах на должности.
ПЗ13 Современные методы подбора кадров.
ПЗ14 Метод компьютерного анализа личности
ПЗ15 Профильный метод анализа личности

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 ЛПЗ по дисциплине

Приложение3

Перечень вопросов для устного опроса

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

Темы	Номера вопросов
Тема 2.4. Организационные основы и принципы деятельности подразделений защиты информации	1-5
Тема 2.5. Подбор, расстановка и обучение сотрудников подразделений защиты информации	6-11
Тема 2.6. Организация труда сотрудников подразделений защиты информации	11-16
Тема 2.7. Принципы и методы управления подразделений защиты информации	17-18
Тема 2.8. Технология управления подразделениями защиты информации	19-22

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Назовите основные виды угроз безопасности предприятия.
2. Перечислите цель и задачи системы безопасности предприятия.
3. Какие средства используются для обеспечения безопасности предприятия?
4. Дайте определение трем видам правомерного овладения конфиденциальной информацией.
5. Определите в процентах степень опасности внутренних и внешних угроз неправомерному овладению информацией.
6. Какие компоненты входят в состав концептуальной модели безопасности информации?
7. Назовите основные принципы построения системы безопасности предприятия?
8. Какими инструкциями руководствуются при организации работы службы безопасности предприятия?
9. Назвать основные виды безопасности на предприятии.
10. Что необходимо включать в коллективный договор для правового обеспечения защиты информации?
11. Перечислить основные нормативные документы, регламентирующие деятельность в области защиты информации.
12. В чем состоит суть лицензирования деятельности предприятий в области защиты информации?
13. Какие виды деятельности предприятия в области защиты информации необходимо лицензировать?
14. Назвать разделы устава службы безопасности предприятии и дать им характеристику.
15. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.

16. Назначение организационного проектирования (три задачи).
17. Назовите основные этапы проектирования функциональной управленческой деятельности.
18. В чем состоит суть проектирования организационной структуры системы управления?
19. Какие виды документов разрабатываются при организационном проектировании систем управления?
20. Опишите типовое содержание положения о функциональных структурах подразделения.
21. Что должно быть включено в должностные инструкции работников системы управления?
22. Какие подразделения входят в состав СБП?

Приложение 4

Перечень самостоятельных работ:

СР1.1. Подготовка к практическим занятиям, оформление отчета по ПЗ
СР1.2. Презентация на тему: «Статус подразделения защиты информации в структуре предприятия.»
СР1.3. Организационные, технологические и координационные задачи и функции (сравнительный анализ).
СР1.4 Виды организационных структур подразделений защиты информации (презентация).
СР1.5. Ответственность заместителя руководителя предприятия по безопасности в области защиты информации (доклад).
Курсовая работа

Примерный перечень тем курсовой работы

1. Комплексный подход к построению технической защиты информации.
2. Основные положения и принципы построения технической защиты информации.
3. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.
4. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
5. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
6. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
7. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.
8. Методы и технические средства съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.
9. Технические средства подслушивания, методы и средства противодействия средствам подслушивания.
10. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере объекта информатизации.
11. Порядок проведения работ по созданию системы защиты информации для объекта информатизации.
12. Организационные методы контроля эффективности защиты информации на примере объекта информатизации.
13. Технические средства контроля эффективности защиты информации на примере объекта информатизации.
14. Разработка предложений по выбору технических средств системы контроля и управления доступом для защиты информации предприятия.
15. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой.
16. Разработка методики защиты персональных данных на предприятии и ее реализация.
17. Разработка предложений по проведению аудита информационной безопасности информационно-вычислительных систем организаций финансово-кредитной сферы.
18. Разработка предложений по защите мультимедийной продукции от

несанкционированного копирования.

19. Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном
20. Сравнительный анализ систем обнаружения и предотвращения компьютерных атак.

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