Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОП. 08 Организационно-правовое обеспечение информационной безопасности

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Белгород 2020 г.

Комплект контрольно-оценочных средств учебной дисциплины разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем** и примерной основной образовательной программы Федерального учебно-методического объединения в системе СПО по укрупненным группам профессий, специальностей **10.00.00 Информационная безопасность** квалификация техник по защите информации (Организация разработчик: **Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность»**, 2017 год).

Рассмотрено цикловой комиссией Протокол заседания № 1 от «31» августа 2020 г. Председатель цикловой комиссии _____/ Чобану Л.А. /	Согласовано Зам.директора по УМР _____/Бакалова Е.Е. «31» августа 2020 г.	Утверждаю Зам.директора по УР _____ /Выручаева Н.В. «31» августа 2020 г.
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2021г. Председатель цикловой комиссии _____/ _____/		
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2022 г. Председатель цикловой комиссии _____/ _____/		
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2023 г. Председатель цикловой комиссии _____/ _____/		

Организация разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородского индустриального колледж»
Петрушин С.Д.
Рецензент *(внутренний):*
преподаватель ОГАПОУ «Белгородский индустриальный колледж»
Чобану Л.А.

1. Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП. 08 Организационно-правовое обеспечение информационной безопасности.

КОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачёта.

КОС разработан на основании:

- положений «Об учебно-методическом комплексе дисциплины, ПМ», «О фонде оценочных средств по дисциплине, профессиональному модулю и основной профессиональной образовательной программе», «О промежуточной аттестации»;
- рабочей программы дисциплины ОП. 08 Организационно-правовое обеспечение информационной безопасности;
- ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Результаты освоения	Основные показатели оценки результата и их критерии	Тип задания; № задания	Форма аттестации (в соответствии с учебным планом)	
			Текущий контроль	**Промежуточная аттестация**
У. 1. Осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;	***Показатель:*** формирование организационных и правовых мер по обеспечению информационной безопасности. ***Критерий:*** точно и обоснованно формирует организационные и правовые меры по обеспечению информационной безопасности, выполнены согласно МУ ПР 1, 2, 3, 4, 5, 6, 7.	**Практические задания**	**ПР 1, 2, 3, 4, 5, 6, 7**	**Дифференцированный зачёт**
У. 2. Применять нормативные правовые акты и нормативные методические документы в области защиты информации;	***Показатель:*** применение правил и законов в области защиты информации. ***Критерий:*** выбор способа и методов применения нормативно правовые актов в области защиты информации, выполнены согласно МУ ПР 1, 2, 3, 4, 5, 6, 7.	**Практические задания**	**ПР 1, 2, 3, 4, 5, 6, 7**	
У. 3. Выявлять каналы утечки информации на объекте защиты;	***Показатель:*** выявлены каналы утечки для различных ситуаций; ***Критерий:*** точно и обоснованно выявлены каналы утечки для различных ситуаций, выполнены согласно МУ ПР 3, 4, 5, 7,	**Практические задания**	**ПР 3, 4, 5, 7**	

У. 4. Контролировать соблюдение персоналом требований режима защиты информации;	***Показатель:*** определение мер для соблюдения персоналом требований режима защиты информации. ***Критерий:*** корректно и обосновано определены меры для соблюдения персоналом требований режима защиты информации, выполнены согласно МУ ПР 1, 2, 3, 4, 5, 7.	**Практические задания**	**ПР 1, 2, 3, 4, 5, 7**
У. 5. Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;	***Показатель:*** оформление документации по регламентации мероприятий и оказанию услуг в области защиты информации. ***Критерий:*** определены и корректно оформлены документы по регламентации мероприятий и оказанию услуг в области защиты информации, выполнены согласно МУ ПР 1, 2, 3, 4, 5, 6, 7.	**Практические задания**	**ПР 1, 2, 3, 4, 5, 6, 7**
У. 6. Защищать свои права в соответствии с трудовым законодательством;	***Показатель:*** определение прав в соответствии с трудовым законодательством. ***Критерий:*** корректно определены и описаны права в соответствии с трудовым законодательством, выполнены согласно МУ ПР 3, 7.	**Практические задания**	**ПР 3, 7**
З. 1. Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	***Показатель:*** описание основных нормативно правовых актов в области информационной безопасности и защиты информации. ***Критерий:*** корректно и в полной мере описаны основные нормативно-правовые акты в области информационной безопасности и защиты информации в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**

3. 1. Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	***Показатель:*** описание основных нормативно правовых актов в области информационной безопасности и защиты информации. ***Критерий:*** корректно и в полной мере описаны основные нормативно-правовые акты в области информационной безопасности и защиты информации в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**
3. 2. Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;	***Показатель:*** описаны правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны. ***Критерий:*** описано полно правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**
3. 3. Правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации	***Показатель:*** описаны правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. ***Критерий:*** полно и точно описаны правовые нормы и стандарты в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**

средств защиты информации;			
З. 4. Организацию ремонтного обслуживания аппаратуры и средств защиты информации;	***Показатель:*** описание процедуры ремонтного обслуживания аппаратуры с точки зрения организации защиты информации. ***Критерий:*** подробно описаны процедуры ремонтного обслуживания аппаратуры с точки зрения организации защиты информации в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**
З. 5. Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;	***Показатель:*** перечислены принципы и методы организационной защиты информации. ***Критерий:*** точно перечислены и подробно охарактеризованы принципы и методы организационной защиты информации, выполнены согласно МУ ПР 7.	**Практические задания**	**устный опрос** **защита практических работ**
З. 6. Правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);	***Показатель:*** описание правового положения субъектов правоотношений в сфере профессиональной деятельности. ***Критерий:*** точно и подробно охарактеризована правовое положение субъектов правоотношений в сфере профессиональной деятельности в соответствии с учебно-методической литературой	**Теоретические задания**	**устный опрос** **защита практических работ**

2. Комплект оценочных средств

2.1. Промежуточная аттестация

В соответствии с учебным планом специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем** формой промежуточной аттестации является дифференцированный зачёт.

Дифференцированный зачёт выставляется на основании:

1. Выполнения и защиты всех практических работ.
2. Наличие всех конспектов лекций.
3. Результатов ежемесячных аттестаций.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены все практические работы и защищены на 5, средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены все практические работы и защищены на 4, средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены все практические работы и защищены на 3, средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются на все конспекты лекции, обучающимися не выполнены все практические работы, средний балл по аттестациям ниже 2,5.

2.2 Текущий контроль

Учебным планом специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем по дисциплине Организационно-правовое обеспечение информационной безопасности предусмотрено проведение практических работ в объеме 30 часов.

2.2.1 Список тем практических работ

1. Работа с нормативными документами
2. Защита информации, содержащейся в информационных системах общего пользования
3. Разработка базового блока документов для обеспечения информационной безопасности ИСПДН
4. Подготовка документов к получению лицензии
5. Подготовки документов к сертификации
6. Подготовка документов к аттестации объектов информатизации
7. Составление трудового договора сотрудника службы информационной безопасности

2.2.2 Условия выполнения практических работ

Методические указания для проведения практических работ (Приложение 1) состоят из:

- Теоретической части, где систематизированы основные теоретические понятия необходимые для проведения работы;
- Практической части, где сформулированы задания, которые необходимо выполнить в ходе работы;

Для успешного выполнения практического занятия студент должен ознакомиться с теоретической частью, примерами и условиям выполнения заданий. По окончании работы студент должен оформить отчет о ее выполнении. Отчет должен быть сдан на следующем занятии.

Время выполнения практических работ определяется рабочей программой дисциплины и календарно-тематическим планом. В аудитории практические работы выполняются студентами индивидуально или в подгруппах, оформление отчета о выполнения работы проводится индивидуально или в подгруппах. В случае отсутствия студента во время проведения практической работы предполагается дополнительная устная защита отчета при его сдаче, с возможным требованием демонстрации выполнения одного и/или нескольких практических заданий (на усмотрение преподавателя).

2.2.3 Критерии оценки практических работ

Оценка «отлично»: правильно выполнены все задания практической части практической работы, правильно даны ответы на все контрольные вопросы, своевременно предоставлен отчет о выполнении работы.

Оценка «хорошо»: правильно выполнены все задания практической части практической работы, правильно даны ответы на большую часть контрольных вопросов, несвоевременно предоставлен отчет о выполнении работы, либо в случае своевременного предоставления отчета, но с наличием несущественных ошибок в выполнении практических заданий и/или ответах на контрольные вопросы, не противоречащих основным понятиям дисциплины.

Оценка «удовлетворительно»: выполнены не все, но более 50% заданий практической работы, дан ответ на часть контрольных вопросов, имеются несущественные ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, не противоречащие основным понятиям дисциплины, несвоевременно предоставлен отчет о выполнении работы.

Оценка «неудовлетворительно»: выполнено менее 50% практических заданий практической части работы, не даны ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, отчет о выполнении работы не предоставлен.

3. Пример теоретических и практических заданий

Теоретические вопросы

1. Объясните назначение справочных систем типа «КонсультантПлюс».
2. Перечислите компоненты меню стартовой страницы.
3. В чем заключается польза путеводителей? Какой из путеводителей вы будете использовать при ведении поиска информации, связанной с информационной безопасностью?
4. Что такое карточка поиска?
5. В каких случаях используется совместная работа быстрого поиска и правового навигатора?
6. Опишите поиск фрагмента текста.
7. Расскажите о назначении «умных ссылок».

8. Перечислите ряд первоочередных мер по предотвращению угроз национальным интересам.

9. Какие вы можете назвать способы сохранения собранной информации?

10. Для каких целей используются закладки?

11. Поясните принцип работы истории поисков.

Практические задания:

Задание 1. Используя «Руководство пользователя» (РК) по работе со справочной правовой системой «КонсультантПлюс», познакомиться со структурой интерфейса программы, процессами запуска системы, назначением вкладок.

Задание 2. Найти ФЗ-152.

Задание 3. Найти статьи УК РФ, относящиеся к правонарушениям в сфере информационных технологий.

Задание 4. Определите дату принятия Доктрины информационной безопасности РФ.

Задание 5. Найти информацию о наказании за разработку вредоносного программного обеспечения.

Задание 6. Найти последний законодательный акт, принятый в сфере информационной безопасности.

Задание 7. Найти статью «Правовая защита цифрового контента от пиратства в сети Интернет и ее влияние на развитие телевизионной и киноотрасли».

Задание 8. Провести сравнение редакций закона «О связи».

Задание 9. Найти форму приказа на увольнение.