ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники
Кафедра «Информационная безопасность»

# ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

## Б1.О.07 «Введение в профессиональную деятельность»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: № 8 Разработка автоматизированных систем в защищенном исполнении

ОПОП по специальности:

Информационная безопасность автоматизированных систем

Квалификация выпускника: специалист по защите информации

Форма обучения - очная
Срок обучения — 5,5 лет

Рязань 2023 г.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

Промежуточный контроль по дисциплине осуществляется проведением теоретического зачета.

## 2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

| № п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции (или её части) | Вид, метод, форма оценочного мероприятия |
|---|---|---|---|
| | Введение | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |
| | Требования образовательного стандарта к профессиональным знаниям, умениям и опыту специалиста | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |
| | Информационная | УК-4 (УК-4.6); УК-6 | зачет |

| | | | |
|---|---|---|---|
| | безопасность, история, основные понятия и правовые основы | (УК-6.1; УК-6.2; УК-6.3) | |
| | Технические средства разведки | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |
| | Организационные основы и методологические принципы защиты информации | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |
| | Методы защиты информации | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |
| | Мероприятия по выявлению технических каналов утечки информации | УК-4 (УК-4.6); УК-6 (УК-6.1; УК-6.2; УК-6.3) | зачет |

## 3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

**Уровень освоения компетенций, формируемых дисциплиной:**

*а) описание критериев и шкалы оценивания тестирования:*

| Шкала оценивания | Критерий |
|---|---|
| 3 балла (эталонный уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100% |
| 2 балла | уровень усвоения материала, предусмотренного |

| | |
|---|---|
| (продвинутый уровень) | программой: процент верных ответов на тестовые вопросы от 70 до 84% |
| 1 балл (пороговый уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69% |
| 0 баллов | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49% |

*б) описание критериев и шкалы оценивания теоретического вопроса:*

| **Шкала оценивания** | **Критерий** |
|---|---|
| 3 балла (эталонный уровень) | выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя |
| 2 балла (продвинутый уровень) | выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов |
| 1 балл (пороговый уровень) | выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя |
| 0 баллов | выставляется студенту, который не смог ответить на вопрос |

На промежуточную аттестацию (зачет) выносится тест (10 вопросов), два теоретических вопроса. Максимально студент может набрать 10 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «зачтено», «не зачтено».

## 4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

### *4.1. Промежуточная аттестация (зачет)*

| Коды компетенций/ и индикаторов | Результаты освоения ОПОП<br>Содержание компетенций/ индикаторов |
|---|---|
| УК-4<br>(УК-4.6) | **Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия**<br><br>***УК-4.6 Представляет свою профессиональную деятельность и может поддержать разговор при ее обсуждении*** |

***а) типовые тестовые вопросы:***

1. Перечислите виды информации в зависимости от категории доступа к ней:
- общедоступная и ограниченного доступа. Информация ограниченного доступа делится на конфиденциальные данные и государственную тайну.

2. Виды информации по назначению:

+а) массовая

+б) личная

г) распространяемая

д) служебная тайна

3. Дайте определение понятия «персональные данные»:

**Персональные данные** – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

4. Назовите типы профессий по целям:

по целям различают гностические (эксперт, ревизор), преобразующие (токарь, строитель) и изыскательские (исследователь, научный работник).

5. Назовите типы профессий, различаемых по средствам труда.

По средствам труда различают профессии, где доминирует ручной труд (представители народных промыслов), механизированный труд (машинист, водитель) и автоматизированный труд (оператор).

6. Дайте определение понятия профессиональная пригодность:

Профессиональная пригодность – это вероятностная характеристика, отражающая возможности человека по овладению какой-либо профессиональной деятельностью.

7. Перечислите структурные компоненты, определяющие пригодность человека к работе:

структурными компонентами пригодности человека к работе являются:

– гражданские качества (моральный облик, отношение к обществу); в некоторых профессиях, например, судья, политик недостаточное развитие именно этих качеств делает человека профессионально непригодным;

– отношение к труду (интересы и склонности к данной области трудовой деятельности);

– общая дееспособность (широта и глубина ума, самодисциплина, самоконтроль, активность и т.д.);

– специальные способности (память на ароматы, музыкальный слух, пространственное мышление и т.д.);

– знания, навыки, опыт в данной профессиональной области.

8. Перечислите тенденции развития системы высшего технического образования.

Общими тенденциями развития системы высшего технического образования являются:

– многоуровневость и преемственность профессиональной подготовки;

– унификация образовательных программ базового уровня и индивидуализация программ высшего уровня;

– интеграция учебной, исследовательской и производственной деятельности студентов в процессе подготовки;

– снижение аудиторной нагрузки и увеличение доли самостоятельной работы, формирование навыков непрерывного самообразования;

– широкое использование в учебном процессе возможностей современных информационных и телекоммуникационных технологий;

– разработка индивидуальных образовательных траекторий обучения с учетом пихофизиологических особенностей студентов;

– нацеленность на формирование готовности выпускников к творческой профессиональной деятельности.

9. Что является организационно-юридической основой для проектирования и унифицирования содержания и показателей качества подготовки специалистов:

+ а) государственные образовательные стандарты высшего профессионального образования

б) учебный план специальности

в) рабочие программы дисциплин

г) основная профессиональная образовательная программа по специальности

9. Виды инженерной деятельности:

+а) производственно-технологическая

б) административная

в) управленческая

г) конструкторская

10. Какие компетенции относятся к общепрофессиональным:

а) способность проводить анализ защищенности автоматизированных систем

б) способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности

+в) способность использовать нормативные правовые документы в своей профессиональной деятельности

г) способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

11. Что является объектом профессиональной деятельности специалиста по информационной безопасности:

+а) объекты информатизации, включая компьютерные

б) промышленные объекты

в) программные продукты

+г) процессы управления информационной безопасностью защищаемых объектов

12. Задачи, решаемые специалистом по защите информации:

а) администрирование вычислительных сетей

б) установка, настройка и обслуживание систем управления базами данных

в) обслуживание операционных систем

+г) администрирование подсистем информационной безопасности объекта

13. Принципы построения комплексной системы защиты информации

+а) принцип персональной ответственности за защиту информации

+б) принцип непрерывности

+ в) принцип обоснованности защиты информации

+г) принцип гибкости

14. Основу политики безопасности составляет

а) наиболее важные субъекты доступа

б) наиболее важные объекты доступа

+в) способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы

г) способ взаимодействия субъектов системы с объектами системы

15. Требования, предъявляемые к комплексной системе защиты информации:

а) она должна быть непротиворечивой

б) она должна быть однозначной

в) она должна быть прозрачной

+г) она должна быть всеохватывающей.

16. Организационные требования к системе защиты

а) управленческие и идентификационные

б) административные и аппаратурные

+ в) административные и процедурные

г) аппаратурные и физические

17. Надежность СЗИ определяется

а) усредненным показателем

+ б) самым слабым звеном

в) количеством отраженных атак

г) самым сильным звеном

18. Если средство защиты способно противостоять отдельным атакам, то согласно «Европейским критериям» безопасность считается

а) низкой

б) средней

в) стандартной

+ г) базовой

19. Перечислите пункты постулата системы защиты:

1. система защиты информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая;

2. никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

3. никакую систему защиты нельзя считать абсолютно надежной, т.к. всегда может найтись злоумышленник, который найдет лазейку для доступа к информации (действия злоумышленника всегда носят комплексный характер, т.к. он любыми средствами стремится добыть важную информацию);

4. система защиты должна быть адаптируемой (приспособляющейся) к изменяющимся условиям.

20. Выберите стратегии защиты:

+ а) оборонительная

б) сдерживающая
+в) упреждающая
г) отслеживающая

***б) типовые теоретические вопросы:***

1. Виды информации по категориям доступа. Общедоступная информация и информация и информация ограниченного доступа. Конфиденциальная информация.
2. Основные нормативно-правовые акты, регулирующие отношения в сфере защиты информации в России.
3. Требования ФГОС ВО к выпускнику и подготовка по ООП.
4. Требования образовательного стандарта к профессиональным знаниям, умениям и опыту специалиста.
5. Объекты профессиональной деятельности специалиста по информационной безопасности.
6. Виды профессиональной деятельности.
7. Сущность и задачи комплексной системы защиты информации.
8. Принципы построения комплексной системы защиты информации.
9. Стратегии защиты информации.
10. Разработка политики безопасности предприятия.

| **Коды компетенций/ и индикаторов** | **Результаты освоения ОПОП**<br>**Содержание компетенций/ индикаторов** |
|---|---|
| УК-6.<br>(УК-6.1.<br>УК-6.2<br>УК-6.3) | **Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни**<br><br>***УК-6.1.Понимает процесс развития средств защиты информации и изучает их для последующего использования в работе.***<br><br>***УК-6.2 Понимает тенденции развития в области защиты информации и необходимость их самостоятельного изучения.***<br><br>***УК-6.3 Понимает тенденции развития в области защиты информации и выбирает и изучает из них наиболее*** |

| | |
|---|---|
| | ***приоритетные*** |

***в) типовые тестовые вопросы:***

1. Преднамеренной угрозой безопасности информации является

+ а) несанкционированное копирование конфиденциальной информации

б) наводнение

в) повреждение кабеля, по которому идет передача, в связи с погодными условиями

г) ошибка администратора

2. НЕпреднамеренной угрозой безопасности информации является

+ а) повреждение кабеля, по которому идет передача, в связи с погодными условиями

б) кража

в) умышленная порча носителей информации

г) несанкционированное копирование конфиденциальной информации

3. Политика безопасности - это

а) набор настроек средств защиты информации

+б) набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение конфиденциальной информации в системе

в) система защиты конфиденциальной информации

г) информация о настройках средств защиты информации

4. Процесс разработки политики безопасности включает в себя

а) поиск уязвимостей в автоматизированной системе

+ б) комплекс мероприятий, связанных с проведением анализа рисков.

в) мероприятия по настройке средств защиты информации в соответствии с результатами анализа рисков

+г) мероприятия по оценке соответствия мер по обеспечению защиты информации системы некоторому эталонному образцу

5. Адаптивная безопасность сети обеспечивается следующими из предложенных элементами: (1) технологиями анализа защищенности, (2) технологиями обнаружения атак, (3) технологиями управления рисками

+ а) 1,2,3

б) 2

в) 1,3

г) ничем из перечисленного

6. В настоящее время применяются следующие модели политик безопасности:

+а) избирательная

+ б) полномочная

+в) мандатная

+г) дискреционная

+д) многоуровневая

7. Избирательная политика безопасности строится на основе

+а) прав доступа субъекта к объекту системы

б) мандатных меток субъектов и объектов системы

в) информационных потоков системы

г) потоков управляющей информации в системе.

8. Избирательное управление доступом реализует принцип

а) все разрешено

+ б) что не разрешено, то запрещено

в) что не запрещено, то разрешено

г) запрещено то, что не используется

9. Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

+а) системном

б) сетевом

в) внешнем

г) приложений

9. Защищаемый объект информатизации – это

а) Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, и технических средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией

б) Совокупность информационных ресурсов, содержащих сведения ограниченного доступа, технических средств и систем обработки информации ограниченного доступа, используемых в соответствии с заданной информационной технологией, и технических средств обеспечения объекта информатизации

+ в) объект информатизации предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

г) Совокупность технических средств и систем обработки информации ограниченного доступа, технических средств обеспечения объекта информатизации, а также помещений или объектов (зданий, сооружений, технических средств), в которых они установлены

10. Контролируемая зона - это

а) Охраняемая территория

+ б) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

в) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска.

г) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц.

11. Утечка информации – это

а) Неправомерное разглашение или распространение сведений ограниченного доступа.

б) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

в) Неконтролируемое распространение защищаемой информации в результате несанкционированного доступа к ней

+ г) Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

12. Технический канал утечки информации:

а) Получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации.

б) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками.

в) Получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации

+г) Совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

13. Вспомогательные технические средства и системы - это

а) технические средства и системы, включая соединительные линии и кабели питания, используемые для обработки, передачи и хранения информации ограниченного доступа.

б) совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и технических средств, которыми добывается защищаемая информация.

в) то технические средства и системы, которые размещаются в тех же помещениях, где и объект информатизации, и участвующие в процессе обработки информации ограниченного доступа

+ г) то технические средства и системы, которые размещаются в тех же помещениях, где и объект информатизации, но не участвующие в процессе обработки информации ограниченного доступа

14. К основным техническим средствам и системам могут относиться:

а) системы радиовещания

б) системы кондиционирования

+ в) системы звукозаписи и звукоусиления

г) офисная техника (компьютеры, принтеры, копиры и т.д.)

15. К вспомогательным средствам и системам могут относиться:

а) средства вычислительной техники

+ б) оконечные устройства телефонной связи

в) информационные системы

г) средства тиражирования документов

16. Организационные требования к системе защиты

а) управленческие и идентификационные

б) административные и аппаратурные

+ в) административные и процедурные

г) аппаратурные и физические

17. Требования к техническому обеспечению системы защиты

а) управленческие и документарные

+ б) аппаратурные и физические

в) процедурные и раздельные

г) административные и аппаратурные

18. Применение средств защиты физического уровня ограничивается услугами

а) целостности

б) аутентификации

в) контроля доступа

+ г) конфиденциальности

***г) типовые теоретические вопросы:***

1. Сущность и задачи комплексной системы защиты информации
2. Принципы построения комплексной системы защиты информации
3. Цели системного подхода к защите информации.
4. Стратегии защиты информации
5. Разработка политики безопасности предприятия

6. Основные требования, предъявляемые к комплексной системе защиты информации.
7. Теоретические основы защиты информации. Концепция информационной безопасности
8. Методологические принципы защиты информации.
9. Корпоративная политика информационной безопасности и защиты информации.
10. Состав и структура системы обеспечения информационной безопасности Российской Федерации.

### *4.2. Типовые задания и вопросы для зачета по дисциплине (сводный список)*

1. Теоретические основы защиты информации.
2. Понятие концепции информационной безопасности
3. Перечислите общетеоретические принципы защиты информации
4. Какие методологические принципы защиты информации вы знаете?
5. Перечислите уровни концепции защиты информации
6. Перечислите правовые принципы защиты информации
7. Какие организационные принципы защиты информации вы знаете?
8. Принципы, используемые при защите информации от технических средств разведки
9. Какие нормативные акты лежат в основе государственной политики обеспечения информационной безопасности?
10. Какие функции выполняет государство по обеспечению информационной безопасности.
11. Какие документы регламентируют деятельность по лицензированию в области технической защиты информации?
12. Какие документы регламентируют деятельность по лицензированию в области криптографической защиты информации?
13. Государственная система аттестации объектов информатизации
14. Виды системы аттестации объектов информатизации.
15. Основные виды информационных угроз
16. Основные методы защиты корпоративных сетей
17. Обнаружение атак.
18. Электронная подпись.
19. Системы антивирусной защиты.
20. Состав и структура системы обеспечения информационной безопасности Российской Федерации (СОИБ РФ).

21. Состав СОИБ РФ
22. Основные элементы организационной основы СОИБ РФ.
23. Принципы обеспечения безопасности
24. Функции системы безопасности
25. Силы обеспечения информационной безопасности РФ
26. Функции ФСБ по защите информации
27. Функции Федеральной Службы по техническому и экспортному контролю РФ в области защиты информации
28. Функции Федерального агентства по техническому регулированию и метрологии
29. Силы и средства обеспечения безопасности Российской Федерации
30. Органы федеральной службы безопасности.

Составил
старший преподаватель кафедры
«Информационная безопасность» Т.И. Калинкина