



ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ИНСТИТУТ ПСИХОЛОГИИ

**Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ ИНСТИТУТ ПСИХОЛОГИИ»
(ОЧУ ВО «МИП»)**

ОДОБРЕНА:

на заседании Ученого совета
Протокол № 3 от «26» марта 2026 г.

УТВЕРЖДАЮ:



Ректор ОЧУ ВО «МИП»
В.В. Столяренко
«26» марта 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.30 Информационная безопасность

основной профессиональной образовательной программы высшего образования - программы бакалавриата по направлению подготовки 09.03.03 Прикладная информатика направленность (профиль) программы бакалавриата - «Прикладные информационные технологии в психологическом консультировании»

(форма обучения: очно-заочная)
(в том числе, **типовые оценочные материалы**
для проведения текущего контроля успеваемости
и промежуточной аттестации обучающихся по дисциплине)

Год набора - 2027

Москва, 2026

Рабочая программа учебной дисциплины Б1.О.30 Информационная безопасность является компонентом основной профессиональной образовательной программы высшего образования - программы бакалавриата по направлению подготовки 09.03.03 Прикладная информатика (направленность (профиль) программы бакалавриата - «Прикладные информационные технологии в психологическом консультировании», форма обучения - очно-заочная).

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденного приказом Министерства образования и науки РФ от 19.09.2017 г. № 922 (зарегистрирован Минюстом России 12.10.2017 № 48531) (в редакции приказов Минобрнауки России от 26.11.2020 № 1456, от 08.02.2021 № 83, от 19.07.2022 № 662, от 27.02.2023 № 208) (ФГОС ВО 3++).

Рабочая программа дисциплины разработана с учетом рабочей программы воспитания, календарного плана воспитательной работы Института, утвержденных ректором Института.

Рабочая программа дисциплины в актуальной редакции рассмотрена на заседании кафедры «Психологии и гуманитарных дисциплин» (протокол № 2 от 19.03.2026), одобрена на заседании Ученого совета (протокол № 3 от 26.03.2026 г.) и утверждена ректором Образовательного частного учреждения высшего образования «Московский институт психологии» (ОЧУ ВО «МИП») 26.03.2026 г.

Оглавление

1. Наименование и цель освоения дисциплины	5
2. Место дисциплины в структуре образовательной программы	5
3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.....	6
4. Объем и содержание дисциплины	7
4.1. Общая трудоемкость дисциплины	7
4.2. Распределение учебного времени по темам и видам учебных занятий	7
очно-заочная форма обучения	7
4.3. Содержание дисциплины, структурированное по темам (разделам)	10
4.4. Дидактические единицы (вопросы) для подготовки к практическим занятиям, контроля и самоконтроля знаний теоретического материала по пройденным темам	13
4.5. Примерный перечень вопросов для организации и планирования самостоятельной работы студентов по изученным темам/разделам	19
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	20
6. Обучение инвалидов и лиц с ограниченными возможностями здоровья	22
7. Организация воспитательной работы в процессе реализации дисциплины как компонента образовательной программы	23
8. Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)	23
8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).....	23
8.2. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины (модуля)	24
8.3. Электронно-библиотечные системы.....	24
8.4. Перечень комплектов лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, используемого при изучении учебной дисциплины (модуля)	24
8.5. Современные профессиональные базы данных и информационно-справочные системы	25
8.6. Материально-техническое обеспечение дисциплины.....	25
9. Методические материалы, определяющие процедуры оценивания результатов обучения	27
9.1. Описание оценочных средств текущего, рубежного и промежуточного контроля	28
9.2. Формы текущего/рубежного контроля успеваемости и достижения результатов обучения.....	29
9.3. Критерии оценки результатов текущего и рубежного контроля	31
9.4. Процедура промежуточной аттестации	33
9.5. Критерии оценки образовательных результатов обучающихся на экзамене по дисциплине:	33
9.6. Соответствие уровня освоения компетенции планиваемым результатам обучения и критериям их оценивания	34
10. Оценочные средства для проведения контроля успеваемости и промежуточной аттестации обучающихся по дисциплине	36

10.1. Типовые контрольные задания для проведения текущей/рубежной аттестации по дисциплине (модулю).....	37
10.2. Примерный перечень тестовых заданий для текущего/рубежного/промежуточного контроля.....	39

1. Наименование и цель освоения дисциплины

Учебная дисциплина «Информационная безопасность» изучается обучающимися, осваивающими образовательную программу «Прикладные информационные технологии в психологическом консультировании» по направлению подготовки 09.03.03 Прикладная информатика.

Основная цель изучения учебной дисциплины состоит в формировании у обучающихся системы знаний, умений и навыков в области обеспечения информационной безопасности и защиты персональных данных, в том числе сведений о состоянии здоровья и врачебной тайны, при проектировании и эксплуатации прикладных информационных систем.

Задачи дисциплины:

- сформировать знание нормативно-правовой базы информационной безопасности и требований законодательства о персональных данных;
- выработать умение выявлять угрозы и уязвимости, строить модель угроз и определять уровень защищенности информационных систем персональных данных;
- сформировать владение организационными и техническими мерами защиты информации, включая криптографические средства и сертифицированные средства защиты информации.

Дисциплина учитывает требования профессиональных стандартов 06.001 «Программист», 06.015 «Специалист по информационным системам», 06.022 «Системный аналитик», 06.025 «Специалист по дизайну графических и пользовательских интерфейсов».

2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к обязательной части программы бакалавриата по направлению 09.03.03 Прикладная информатика. Реализуется в рамках Блока 1 Дисциплины (модули), изучается на 4 курсе в 7 семестре и завершается экзаменом.

Освоение дисциплины опирается на знания и умения, сформированные при изучении дисциплин «Правоведение» (3 семестр), «Веб-технологии Backend» (5 семестр), «Вычислительные системы, сети и телекоммуникации» (5 семестр), «Операционные системы» (5 семестр).

Одновременно с ней изучаются дисциплины «Этика и регулирование данных в ментальном здоровье» (7 семестр), «Платформы онлайн-консультирования: архитектура и

проектирование» (7 семестр, дисциплина по выбору), с которыми она связана по содержанию.

Результаты освоения дисциплины используются при изучении дисциплин «DevOps и развертывание информационных систем» (8 семестр), «Цифровая психодиагностика и психометрика» (8 семестр), «Мобильная разработка для mental-health сервисов» (8 семестр, дисциплина по выбору), при прохождении практики «Преддипломная практика» (9 семестр), при выполнении и защите выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся по программе бакалавриата должен овладеть:

УК-8 *Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов*

ОПК-3 *Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*

Планируемые результаты обучения по дисциплине

Формируемая компетенция	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Идентифицирует и анализирует опасные и вредные факторы среды обитания и профессиональной деятельности; оценивает риски для жизни и здоровья. УК-8.2. Обеспечивает безопасные условия жизнедеятельности в повседневной жизни и на рабочем месте; соблюдает требования охраны труда и информационной безопасности. УК-8.3. Применяет правила поведения и алгоритмы действий при возникновении чрезвычайных ситуаций природного, техногенного и социального характера, а также в условиях военных конфликтов; оказывает первую помощь.	Знать: основы безопасности жизнедеятельности и охраны окружающей среды; требования законодательства Российской Федерации в области гражданской обороны и защиты от чрезвычайных ситуаций; принципы устойчивого развития; правила оказания первой помощи Уметь: идентифицировать опасные и вредные факторы в быту и профессиональной среде; применять средства индивидуальной и коллективной защиты; действовать в условиях чрезвычайных ситуаций; оказывать первую помощь Владеть: навыками обеспечения безопасности в быту и профессиональной деятельности; приемами

		поведения при чрезвычайных ситуациях и военных конфликтах; методами минимизации негативного воздействия на природную среду
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Применяет профессиональные информационные и библиографические ресурсы, научные базы данных, реестры и справочные системы для решения стандартных задач. ОПК-3.2. Использует информационно-коммуникационные технологии при решении стандартных задач, связанных с проектированием, сопровождением и применением прикладных информационных систем. ОПК-3.3. Соблюдает основные требования информационной безопасности и защиты персональных данных при работе с информацией в профессиональной деятельности.	Знать: основы информационной и библиографической культуры; состав профессиональных информационных ресурсов в сфере информационных технологий; требования Федерального закона № 152-ФЗ «О персональных данных» и основ информационной безопасности Уметь: пользоваться ИКТ и профессиональными информационными ресурсами при решении стандартных задач; оформлять библиографические ссылки и списки литературы; применять базовые меры по защите информации Владеть: навыками работы с профессиональной информацией с учетом требований информационной безопасности; приемами защиты персональных данных и обеспечения конфиденциальности в информационных системах

4. Объем и содержание дисциплины

4.1. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 часов).

№	Семестр	Общая трудоемкость		В том числе контактная работа с преподавателем							Контроль	Сам. работа	Форма промежуточной аттестации
		В з.е.	В часах	всего	Л	Сем	КоР	КРП	Конс	Э			
1	7	6	216	80	28	52	-	-	-	-	36	100	Экзамен
Примечание: В з.е. - в зачетных единицах Л. (Лек.) - лекция Пр. - практическое занятие Сем. - семинар КоР. - контрольная работа КРП - курсовая работа (курсовой проект) СР (Сам.работа) - самостоятельная работа З - зачет/зачет с оценкой К (Конс.) - консультация Э. - экзамен Контроль - контрольное время на подготовку к экзамену													

4.2. Распределение учебного времени по темам и видам учебных занятий

очно-заочная форма обучения

№	Наименование	Всего	Контактная работа с преподавателем	Сам.	Формируемые
---	--------------	-------	------------------------------------	------	-------------

	тем учебных занятий	часов	Всего	Л	Сем	КоР	КРП	Конс	Э	раб.	компетенции
1	Тема 1. Понятие и основы информационной безопасности	8	4	2	2					4	УК-8, ОПК-3
2	Тема 2. Нормативно-правовая база информационной безопасности в Российской Федерации	6	2		2					4	УК-8, ОПК-3
3	Тема 3. Федеральный закон № 152-ФЗ «О персональных данных»	8	4	2	2					4	УК-8, ОПК-3
4	Тема 4. Категории персональных данных	6	2		2					4	УК-8, ОПК-3
5	Тема 5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья	8	4	2	2					4	УК-8, ОПК-3
6	Тема 6. Оператор персональных данных: обязанности и ответственность	6	2		2					4	УК-8, ОПК-3
7	Тема 7. Согласие на обработку персональных данных	8	4	2	2					4	УК-8, ОПК-3
8	Тема 8. Трансграничная передача персональных данных	6	2		2					4	УК-8, ОПК-3
9	Тема 9. Угрозы информационной безопасности и модель нарушителя	8	4	2	2					4	УК-8, ОПК-3
10	Тема 10. Уязвимости и атаки на информационные системы	6	2		2					4	УК-8, ОПК-3
11	Тема 11. Вредоносное программное обеспечение	8	4	2	2					4	УК-8, ОПК-3
12	Тема 12. Социальная инженерия и фишинг	6	2		2					4	УК-8, ОПК-3
13	Тема 13. Криптографические методы защиты информации	8	4	2	2					4	УК-8, ОПК-3

14	Тема 14. Электронная подпись и удостоверяющие центры	6	2		2				4	УК-8, ОПК-3
15	Тема 15. Идентификация, аутентификация и управление доступом	8	4	2	2				4	УК-8, ОПК-3
16	Тема 16. Межсетевые экраны и системы обнаружения вторжений	6	2		2				4	УК-8, ОПК-3
17	Тема 17. Защита информации в компьютерных сетях	8	4	2	2				4	УК-8, ОПК-3
18	Тема 18. Безопасность веб-приложений и мобильных сервисов	6	2		2				4	УК-8, ОПК-3
19	Тема 19. Категорирование информационных систем персональных данных	8	4	2	2				4	УК-8, ОПК-3
20	Тема 20. Определение уровней защищенности информационных систем персональных данных	6	2		2				4	УК-8, ОПК-3
21	Тема 21. Средства защиты информации и их сертификация	8	4	2	2				4	УК-8, ОПК-3
22	Тема 22. Организационные меры защиты информации	6	2		2				4	УК-8, ОПК-3
23	Тема 23. Управление инцидентами информационной безопасности	7	4	2	2				3	УК-8, ОПК-3
24	Тема 24. Резервное копирование и восстановление данных	5	2		2				3	УК-8, ОПК-3
25	Тема 25. Аудит информационной безопасности	7	4	2	2				3	УК-8, ОПК-3
26	Тема 26. Обеспечение без-	7	4	2	2				3	УК-8, ОПК-3

опасности сервисов ментального здоровья: комплексный подход										
Промежуточная аттестация (экзамен)	36									УК-8, ОПК-3
Итого	216	80	28	52					100	

4.3. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Понятие и основы информационной безопасности.

Информация как объект защиты, свойства конфиденциальности, целостности и доступности, понятие угрозы и защиты информации. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 2. Нормативно-правовая база информационной безопасности в Российской Федерации.

Система нормативных актов в области защиты информации: Конституция, 149-ФЗ, 152-ФЗ, 187-ФЗ, приказы ФСТЭК и ФСБ России. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 3. Федеральный закон № 152-ФЗ «О персональных данных».

Основные понятия закона, принципы и условия обработки персональных данных, права субъекта персональных данных. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 4. Категории персональных данных.

Общие, специальные и биометрические персональные данные, особенности обработки сведений о состоянии здоровья. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья.

Правовой режим врачебной тайны, сведения о психическом здоровье, конфиденциальность в цифровых сервисах психологической помощи. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 6. Оператор персональных данных: обязанности и ответственность.

Обязанности оператора, уведомление Роскомнадзора, ответственность за нарушение законодательства о персональных данных. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 7. Согласие на обработку персональных данных.

Формы и содержание согласия, согласие на обработку специальных категорий, отзыв согласия субъектом. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 8. Трансграничная передача персональных данных.

Условия трансграничной передачи, адекватность защиты, локализация баз данных на территории Российской Федерации. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 9. Угрозы информационной безопасности и модель нарушителя.

Классификация угроз, источники угроз, построение модели угроз и модели нарушителя. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 10. Уязвимости и атаки на информационные системы.

Понятие уязвимости, классификация атак, банк данных угроз безопасности информации ФСТЭК России. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 11. Вредоносное программное обеспечение.

Виды вредоносного программного обеспечения, механизмы заражения и распространения, средства антивирусной защиты. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 12. Социальная инженерия и фишинг.

Методы социальной инженерии, фишинг и его разновидности, меры противодействия и обучение пользователей. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 13. Криптографические методы защиты информации.

Симметричное и асимметричное шифрование, хеш-функции, российские криптографические стандарты. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 14. Электронная подпись и удостоверяющие центры.

Виды электронной подписи по 63-ФЗ, инфраструктура удостоверяющих центров, проверка подлинности подписи. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 15. Идентификация, аутентификация и управление доступом.

Модели управления доступом, многофакторная аутентификация, разграничение прав в информационных системах. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 16. Межсетевые экраны и системы обнаружения вторжений.

Функции межсетевых экранов, системы обнаружения и предотвращения вторжений, сегментация сети. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 17. Защита информации в компьютерных сетях.

Защищенные сетевые протоколы, виртуальные частные сети, протокол TLS, безопасность передачи данных. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 18. Безопасность веб-приложений и мобильных сервисов.

Типовые уязвимости веб-приложений, защита программных интерфейсов, безопасность мобильных приложений сервисов ментального здоровья. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 19. Категорирование информационных систем персональных данных.

Порядок отнесения информационных систем персональных данных к категориям, определение типа актуальных угроз, обследование систем. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 20. Определение уровней защищенности информационных систем персональных данных.

Уровни защищенности по постановлению Правительства № 1119, состав мер защиты для каждого уровня. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 21. Средства защиты информации и их сертификация.

Классы средств защиты информации, сертификация ФСТЭК и ФСБ России, применение сертифицированных средств. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 22. Организационные меры защиты информации.

Политика информационной безопасности, регламенты, разграничение ответственности, режим служебной тайны. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 23. Управление инцидентами информационной безопасности.

Выявление, регистрация и реагирование на инциденты, взаимодействие с ГосСОПКА, расследование инцидентов. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 24. Резервное копирование и восстановление данных.

Стратегии резервного копирования, планы обеспечения непрерывности и восстановления, тестирование резервных копий. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 25. Аудит информационной безопасности.

Внутренний и внешний аудит, оценка соответствия требованиям, тестирование на проникновение. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

Тема 26. Обеспечение безопасности сервисов ментального здоровья: комплексный подход.

Проектирование системы защиты цифрового сервиса психологической помощи, защита персональных данных и врачебной тайны, комплекс организационных и технических мер. Рассматриваются нормативные требования, методы и типовые задачи применения темы в профессиональной деятельности.

4.4. Дидактические единицы (вопросы) для подготовки к практическим занятиям, контроля и самоконтроля знаний теоретического материала по пройденным темам

Тема 1. Понятие и основы информационной безопасности.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Понятие и основы информационной безопасности».
2. Методы и процедуры: основные понятия информационной безопасности, триада конфиденциальности, целостности и доступности.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 2. Нормативно-правовая база информационной безопасности в Российской Федерации.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Нормативно-правовая база информационной безопасности в Российской Федерации».
2. Методы и процедуры: структура законодательства об информационной безопасности, полномочия ФСТЭК и ФСБ России.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 3. Федеральный закон № 152-ФЗ «О персональных данных».

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Федеральный закон № 152-ФЗ «О персональных данных»».

2. Методы и процедуры: принципы и условия обработки персональных данных по 152-ФЗ, права субъекта.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 4. Категории персональных данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Категории персональных данных».

2. Методы и процедуры: разграничение категорий персональных данных и условия обработки специальных категорий.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Врачебная тайна и конфиденциальность в сервисах ментального здоровья».

2. Методы и процедуры: правовой режим врачебной тайны и защита сведений о психическом здоровье.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 6. Оператор персональных данных: обязанности и ответственность.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Оператор персональных данных: обязанности и ответственность».

2. Методы и процедуры: обязанности оператора персональных данных и виды ответственности за нарушения.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 7. Согласие на обработку персональных данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Согласие на обработку персональных данных».

2. Методы и процедуры: требования к согласию субъекта и порядок его отзыва.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 8. Трансграничная передача персональных данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Трансграничная передача персональных данных».
2. Методы и процедуры: условия трансграничной передачи и требование локализации баз персональных данных.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 9. Угрозы информационной безопасности и модель нарушителя.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Угрозы информационной безопасности и модель нарушителя».
2. Методы и процедуры: построение модели угроз и модели нарушителя.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 10. Уязвимости и атаки на информационные системы.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Уязвимости и атаки на информационные системы».
2. Методы и процедуры: классификация уязвимостей и атак, работа с банком данных угроз ФСТЭК России.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 11. Вредоносное программное обеспечение.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Вредоносное программное обеспечение».
2. Методы и процедуры: виды вредоносного программного обеспечения и средства антивирусной защиты.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 12. Социальная инженерия и фишинг.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Социальная инженерия и фишинг».
2. Методы и процедуры: методы социальной инженерии и меры противодействия фишингу.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 13. Криптографические методы защиты информации.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Криптографические методы защиты информации».
2. Методы и процедуры: симметричное и асимметричное шифрование, хеш-функции и криптографические стандарты.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 14. Электронная подпись и удостоверяющие центры.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Электронная подпись и удостоверяющие центры».
2. Методы и процедуры: виды электронной подписи по 63-ФЗ и инфраструктура удостоверяющих центров.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 15. Идентификация, аутентификация и управление доступом.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Идентификация, аутентификация и управление доступом».
2. Методы и процедуры: модели управления доступом и многофакторная аутентификация.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 16. Межсетевые экраны и системы обнаружения вторжений.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Межсетевые экраны и системы обнаружения вторжений».
2. Методы и процедуры: межсетевые экраны, системы обнаружения вторжений и сегментация сети.
3. Проверка и интерпретация результата в прикладной задаче.

Тема 17. Защита информации в компьютерных сетях.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Защита информации в компьютерных сетях».
2. Методы и процедуры: защищенные сетевые протоколы, виртуальные частные сети и TLS.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 18. Безопасность веб-приложений и мобильных сервисов.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Безопасность веб-приложений и мобильных сервисов».

2. Методы и процедуры: типовые уязвимости веб-приложений и защита программных интерфейсов.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 19. Категорирование информационных систем персональных данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Категорирование информационных систем персональных данных».

2. Методы и процедуры: порядок категорирования информационных систем персональных данных и определение типа актуальных угроз.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 20. Определение уровней защищенности информационных систем персональных данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Определение уровней защищенности информационных систем персональных данных».

2. Методы и процедуры: определение уровней защищенности по постановлению Правительства № 1119.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 21. Средства защиты информации и их сертификация.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Средства защиты информации и их сертификация».

2. Методы и процедуры: классы средств защиты информации и порядок их сертификации.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 22. Организационные меры защиты информации.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Организационные меры защиты информации».
2. Методы и процедуры: разработка политики информационной безопасности и организационных регламентов.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 23. Управление инцидентами информационной безопасности.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Управление инцидентами информационной безопасности».
2. Методы и процедуры: порядок реагирования на инциденты и взаимодействие с ГосСОПКА.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 24. Резервное копирование и восстановление данных.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Резервное копирование и восстановление данных».
2. Методы и процедуры: стратегии резервного копирования и восстановления данных.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 25. Аудит информационной безопасности.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Аудит информационной безопасности».
2. Методы и процедуры: проведение аудита и оценки соответствия требованиям безопасности.

3. Проверка и интерпретация результата в прикладной задаче.

Тема 26. Обеспечение безопасности сервисов ментального здоровья: комплексный подход.

Время - 2 часа.

Основные вопросы:

1. Основные понятия темы «Обеспечение безопасности сервисов ментального здоровья: комплексный подход».
2. Методы и процедуры: проектирование комплексной системы защиты сервиса ментального здоровья.

3. Проверка и интерпретация результата в прикладной задаче.

4.5. Примерный перечень вопросов для организации и планирования самостоятельной работы студентов по изученным темам/разделам

1. Понятие и основы информационной безопасности: основные определения, требования и типовые задачи.
2. Нормативно-правовая база информационной безопасности в Российской Федерации: основные определения, требования и типовые задачи.
3. Федеральный закон № 152-ФЗ «О персональных данных»: основные определения, требования и типовые задачи.
4. Категории персональных данных: основные определения, требования и типовые задачи.
5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья: основные определения, требования и типовые задачи.
6. Оператор персональных данных: обязанности и ответственность: основные определения, требования и типовые задачи.
7. Согласие на обработку персональных данных: основные определения, требования и типовые задачи.
8. Трансграничная передача персональных данных: основные определения, требования и типовые задачи.
9. Угрозы информационной безопасности и модель нарушителя: основные определения, требования и типовые задачи.
10. Уязвимости и атаки на информационные системы: основные определения, требования и типовые задачи.
11. Вредоносное программное обеспечение: основные определения, требования и типовые задачи.
12. Социальная инженерия и фишинг: основные определения, требования и типовые задачи.
13. Криптографические методы защиты информации: основные определения, требования и типовые задачи.
14. Электронная подпись и удостоверяющие центры: основные определения, требования и типовые задачи.
15. Идентификация, аутентификация и управление доступом: основные определения, требования и типовые задачи.
16. Межсетевые экраны и системы обнаружения вторжений: основные определения, требования и типовые задачи.

17. Защита информации в компьютерных сетях: основные определения, требования и типовые задачи.

18. Безопасность веб-приложений и мобильных сервисов: основные определения, требования и типовые задачи.

19. Категорирование информационных систем персональных данных: основные определения, требования и типовые задачи.

20. Определение уровней защищенности информационных систем персональных данных: основные определения, требования и типовые задачи.

21. Средства защиты информации и их сертификация: основные определения, требования и типовые задачи.

22. Организационные меры защиты информации: основные определения, требования и типовые задачи.

23. Управление инцидентами информационной безопасности: основные определения, требования и типовые задачи.

24. Резервное копирование и восстановление данных: основные определения, требования и типовые задачи.

25. Аудит информационной безопасности: основные определения, требования и типовые задачи.

26. Обеспечение безопасности сервисов ментального здоровья: комплексный подход: основные определения, требования и типовые задачи.

27. Место дисциплины «Информационная безопасность» в решении задач защиты персональных данных.

28. Критерии выбора мер и средств защиты информации и проверка их применимости.

29. Способы оценки эффективности принятых мер защиты информации.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

Самостоятельная работа студентов (СРС, СР) является важным видом учебной и научной деятельности, направленным на развитие самостоятельности, ответственности и организованности, творческого подхода к решению задач учебного и профессионального уровня. Самостоятельная работа - обязательная часть учебного процесса для каждого обучающегося, объем которой определяется учебным планом.

Объем, виды и формы самостоятельной работы студентов при реализации дисциплины, порядок ее организации и контроля определяются ведущим преподавателем в соответствии с Методическими рекомендациями по организации самостоятельной работы обучающихся Института и доводятся до сведения обучающихся.

Основными видами самостоятельной работы обучающихся является:

- изучение теоретического учебного материала на основе конспектов лекций и подготовка к практическим занятиям (повторение ответов на теоретические вопросы к занятиям);

- работа с литературой для подготовки выступлений с докладом (эссе, рефератом), а также изучения учебной литературы по вопросам, отведенным на самостоятельное освоение (при наличии);
- подготовка к устному опросу или письменному тестированию, к контрольной работе;
- самостоятельное выполнение практико-ориентированных заданий

Методические рекомендации при подготовке к аудиторным занятиям

К аудиторным занятиям относятся лекционные занятия и практические (семинарские) занятия.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к промежуточной аттестации. В процессе конспектирования следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

В ходе подготовки к практическому занятию обучающемуся рекомендуется изучить указанную в рабочей программе основную литературу, ознакомиться с дополнительной литературой по теме занятия. Для лучшего понимания содержания программы обучающимся рекомендуется постоянно соотносить знания, получаемые в курсе, с уже накопленными сведениями из области психологии, активно задавать вопросы по изучаемому материалу и принимать участие в обсуждениях на практических занятиях.

При решении практических заданий (задач) обучающемуся рекомендуется предварительно повторить теоретический материал по соответствующей теме (вопросу), выписать алгоритм выполнения аналогичных типов заданий и (или) необходимые формулы; кратко отразить исходное условие задания; привести развернутые пояснения хода решения; проанализировать полученные результаты и сформулировать выводы и (или) рекомендации (при необходимости). При решении кейс-заданий в ответе в дополнение к перечисленному следует четко обозначить ключевые факторы / условия, при наличии / соблюдении которых предложенное решение проблемной кейс-ситуации будет эффективным.

Особой формой контактной работы является самостоятельная работа под руководством преподавателя, которая включает тематическую консультацию по дисциплине рабочего учебного плана соответствующего года обучения или разбор заданий отдельного занятия по соответствующей дисциплине, проводимую еженедельно как индивидуально, так и для мелких групп по утвержденному расписанию. Обучающимся рекомендуется посещать такие занятия по необходимости для обеспечения более эффективной подготовки и качества усвоения учебного материала.

Для лучшего освоения теоретического материала необходимо систематически работать с конспектами лекций, осуществлять аналитическую обработку учебной литературы для самостоятельного изучения (аннотирование, рецензирование, реферирование). Следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие, в особенности по вопросам, выносимым на самостоятельное изучение. Представленные в практическом занятии вопросы опираются на пройденный лекционный материал, поэтому к ним желательно готовиться после изучения материала соответствующих лекций.

Доклад и реферат представляют собой сообщение по заданной теме, с целью внести знания из дополнительной литературы, систематизировать материал, проиллюстрировать примерами, развивать навыки самостоятельной работы с научной литературой, познавательный интерес к научному познанию. Эссе, в отличие от доклада, предполагает наличие рассуждений выступающего по выбранной проблематике, его авторскую позицию, аргументированную синтезом информации из различных учебных и (или) научных источников. Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей.

Готовясь к выступлению с докладом, с эссе или реферативному сообщению, обучающийся может обращаться за методической помощью к преподавателю. Начинать подготовку следует составлением плана (конспекта) выступления по изучаемому материалу (вопросу). Далее следует отобрать всю содержательную часть для презентации и выстроить логическую цепочку представления. Определить виды визуализации (картинки) для отображения их на слайдах в соответствии с логикой, целью и спецификой материала.

Практические советы по подготовке выступления с презентацией:

- согласуйте с преподавателем тему для выступления и подберите актуальную литературу;
- готовьте отдельно: текст доклада, слайды (10-15), раздаточный материал (при необходимости);
- выносите на слайды самую значимую информацию, лучше наглядную (таблицы, схемы и т.п.);
- используйте для презентации сдержанный деловой стиль оформления;
- выступление начинайте с обязательной информации: тема, фамилия и инициалы выступающего;
- соблюдайте структуру выступления в докладе и на презентации: план сообщения; слайды, иллюстрирующие (но не дублирующие) текст выступления; краткие выводы из всего сказанного;
- обязательно указывайте список использованных источников;
- будьте готовы к вопросам по теме выступления;
- соблюдайте тайминг во время выступления: до 7 мин. на выступление и 5 мин.- ответы на вопросы.

Методические рекомендации по подготовке и выполнению контрольной работы

Контрольная работа выступает оценочным средством рубежного контроля знаний, умений и навыков обучающегося, сформированных по итогам изучения модуля или совокупности взаимосвязанных тем дисциплины.

Контрольная работа проводится после завершения изучения тем, входящих в модуль дисциплины, но не реже двух раз в семестр, выполняется студентом самостоятельно, без использования вспомогательных материалов (в том числе учебников или конспектов лекций) в отведенное для этого ограниченное время.

Для подготовки к модульной контрольной работе необходимо повторить теоретический материал лекций и примеры выполнения практических заданий по темам модуля. На контрольной работе необходимо прежде всего внимательно прочитать текст заданий, распределить время на их выполнение и приступить к контрольной работе.

6. Обучение инвалидов и лиц с ограниченными возможностями здоровья

Образовательная деятельность обучающихся из числа инвалидов и лиц с ОВЗ осуществляется в соответствии с Приказом Министерства науки и высшего образования Российской Федерации от 25 апреля 2025 г. № 384 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере науки и высшего образования, а также оказания им при этом необходимой помощи», Методическими рекомендациями по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденными Министерством образования и науки РФ 08.04.2014г. № АК-44/05вн, локальными нормативными актами Института.

В институте образовательная деятельность обучающихся с ОВЗ осуществляется на основе образовательных программ, адаптированных, при необходимости, для обучения указанных лиц, с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

В институте созданы специальные условия для получения образования по образовательным программам обучающимися (бакалаврами) с ОВЗ, которые включают в себя

использование специальных методов обучения и воспитания, электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья, специальные технические средства обучения, предоставление услуг ассистента (при необходимости), оказывающего обучающимся (бакалаврам) необходимую техническую помощь, обеспечение беспрепятственного доступа в здание института и свободное перемещение.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ОВЗ производится с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации на основании просьбы, выраженной в письменной форме.

7. Организация воспитательной работы в процессе реализации дисциплины как компонента образовательной программы

В соответствии с действующим законодательством Российской Федерации, локальными нормативными актами Института в рамках реализации дисциплины осуществляется воспитательная работа, направленная на закрепление духовно-нравственных ценностей и (или) развитие высоконравственной личности, способной в полной мере реализовывать свой потенциал и проявить инициативность в условиях современного общества.

Воспитательная работа в рамках реализации дисциплины «Информационная безопасность» как компонента образовательной программы основана на использовании аксиологического, культурно-исторического, системно-деятельностного и личностно ориентированного подхода с учетом основных принципов воспитания: гуманистической направленности, совместной деятельности участников образовательного процесса, следования нравственному примеру, безопасной жизнедеятельности и инклюзивности.

8. Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная литература:

1. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. - 2-е изд. - Москва : Издательство Юрайт, 2026. - 252 с. - (Высшее образование). - ISBN 978-5-9916-4299-6. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/589902> (дата обращения: 03.08.2026).
2. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2026. - 277 с. - (Высшее образование). - ISBN 978-5-534-16450-3. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/588515> (дата обращения: 03.08.2026).

б) дополнительная литература:

3. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2026. - 357 с. - (Высшее образование). - ISBN 978-5-534-19108-0. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/583236> (дата обращения: 03.08.2026).

8.2. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины (модуля)

Название	Эл.адрес	Режим доступа
Личный кабинет обучающегося ОЧУ ВО «МИП» (СДО на базе LMS Moodle)	https://sdo.mip.institute/	для авторизованных пользователей, из любой точки, где есть Интернет
Федеральный портал «Российское образование»	https://edu.ru/	свободный, из любой точки, где есть Интернет
Национальный открытый университет «ИНТУИТ»	https://intuit.ru/	свободный, из любой точки, где есть Интернет
Национальная платформа «Открытое образование»	https://openedu.ru/	свободный, из любой точки, где есть Интернет
Профессиональное сообщество ИТ-специалистов «Хабр»	https://habr.com/ru/	свободный, из любой точки, где есть Интернет

8.3. Электронно-библиотечные системы

Название	Эл. адрес	Режим доступа
Электронно-библиотечная система ЮРАЙТ	https://urait.ru/	для авторизованных пользователей, из любой точки, где есть Интернет

8.4. Перечень комплектов лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, используемого при изучении учебной дисциплины (модуля)

Название ПО	Характер ПО
операционная система Альт Образование 10	свободно распространяемое отечественное ПО (свободная лицензия)
пакет офисных программ LibreOffice	свободно распространяемое ПО (свободная лицензия)
статистический пакет Jamovi	свободно распространяемое ПО (свободная лицензия)
статистический пакет GNU PSPP	свободно распространяемое ПО (свободная лицензия)
система управления проектами ProjectLibre	свободно распространяемое ПО (свободная лицензия)
архиватор 7-Zip	свободно распространяемое ПО (свободная лицензия)
Яндекс.Браузер	свободно распространяемое отечественное ПО (свободная лицензия)
язык программирования Python 3	свободно распространяемое ПО (свободная лицензия PSF)

среда разработки Visual Studio Code	свободно распространяемое ПО (бесплатная лицензия)
среда разработки PyCharm Community Edition	свободно распространяемое ПО (свободная лицензия Apache 2.0)
система управления версиями Git	свободно распространяемое ПО (свободная лицензия GNU GPL)
система управления базами данных PostgreSQL	свободно распространяемое ПО (свободная лицензия)
средство администрирования баз данных DBeaver Community	свободно распространяемое ПО (свободная лицензия Apache 2.0)
библиотеки Python для анализа данных и машинного обучения NumPy, pandas, scikit-learn	свободно распространяемое ПО (свободные лицензии BSD)
графический редактор GIMP	свободно распространяемое ПО (свободная лицензия GNU GPL)
векторный графический редактор Inkscape	свободно распространяемое ПО (свободная лицензия GNU GPL)
среда контейнеризации Podman	свободно распространяемое ПО (свободная лицензия Apache 2.0)

8.5. Современные профессиональные базы данных и информационно-справочные системы

Название	Эл. адрес	Режим доступа
Национальная библиографическая база данных научного цитирования, научная электронная библиотека eLIBRARY.RU	http://www.elibrary.ru	Ресурс открытого доступа
Интернет-ресурс Российской Государственной Библиотеки	https://www.rsl.ru	Ресурс открытого доступа
Международная реферативная база данных научных изданий Springerlink	https://link.springer.com	Ресурс открытого доступа
Реферативная база зарубежных научных публикаций	https://www.scilit.net/	Ресурс открытого доступа
Научная электронная библиотека (база научных статей) «КиберЛенинка»	https://cyberleninka.ru/	Ресурс открытого доступа
Некоммерческие интернет-версии справочно-правовой информационной системы КонсультантПлюс	https://www.consultant.ru/online/	Ресурс открытого доступа
Информационно-правовой портал справочно-правовой информационной системы Гарант	https://www.garant.ru	Ресурс открытого доступа

8.6. Материально-техническое обеспечение дисциплины

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответ-	Собственность или оперативное управление, хозяйственное ведение, аренда (субаренда), безвозмездное пользование, практическая подготовка	Полное наименование собственника (арендодателя, ссудодателя) объекта недвижимого имущества	Документ - основание возникновения права (реквизиты и срок действия)
-------	--	---	--	---	--	--

			ствии с докумен- тами бюро тех- нической инвен- таризации)			
1	2	3	4	5	6	7
1	Б1.О.30 Инфор- мационная без- опасность	Аудитория 105 Учебная аудитория для проведения учебных занятий лекционного, семи- нарского и практи- ческого типа, груп- повых и индивиду- альных консульта- ций, текущего кон- троля и промежу- точной аттестации, самостоятельной работы обучающихся Специализиро- ванная мебель: пар- та двухместная для обучающегося - 4 шт. (8 мест), рабо- чее место препода- вателя (стол и стул) - 1 шт., стеллаж - 1 шт.; Оборудование и технические сред- ства обучения: мо- ноблок IRU Office 310K2 с доступом к сети «Интернет» - 8 шт., принтер XEROX Phaser 3020 - 1 шт., гарнитура полноразмерная с микрофоном - 8 шт. Программное обес- печение: операци- онная система Альт Образование 10 (свободная лицен- зия), пакет офисных программ LibreOffice (свобод- ная лицензия), ста- тистический пакет Jamovi (свободная лицензия), стати- стический пакет GNU PSPP (свобод- ная лицензия), си- стема управления проектами ProjectLibre (сво- бодная лицензия), архиватор 7-Zip (свободная лицен- зия), Ян- декс.Браузер (сво- бодная лицензия), язык программиро- вания Python 3 (сво- бодная лицензия PSF), среда разра- ботки Visual Studio	117105, Россий- ская Федерация, город Москва, вн.тер.г. муници- пальный округ Донской, шоссе Варшавское, дом 2, помещение 3/1; кадастровый но- мер 77:05:0001020:365 4; Этаж 1, поме- щение III, комната 28 (Аудитория внутренний № 105; 21,8 кв.м.)	Аренда	Автономная не- коммерческая до- полнительного профессионально- го образования «Московская Бизнес Академия» (АНО ДПО «МБА»), ИНН 9725034765, ОГРН 1207700285143	Договор аренды нежилых поме- щений № 20- 03/26 от 20.03.2026 в редакции До- полнительного соглашения № 1 от 18.06.2026; срок аренды 11 месяцев, с 20.03.2026 по 19.02.2027; государственная регистрация договора арен- ды не требуется (пункт 2 статьи 651 ГК РФ)

		Code (бесплатная лицензия), среда разработки PyCharm Community Edition (свободная лицензия Apache 2.0), система управления версиями Git (свободная лицензия GNU GPL), система управления базами данных PostgreSQL (свободная лицензия), средство администрирования баз данных DBeaver Community (свободная лицензия Apache 2.0), библиотеки Python для анализа данных и машинного обучения NumPy, pandas, scikit-learn (свободные лицензии BSD), анализатор сетевого трафика Wireshark (свободная лицензия GNU GPL), средство UML-моделирования Modelio (свободная лицензия GNU GPL), средство криптографической защиты информации VeraCrypt (свободная лицензия), графический редактор GIMP (свободная лицензия GNU GPL), векторный графический редактор Inkscape (свободная лицензия GNU GPL), среда контейнеризации Podman (свободная лицензия Apache 2.0), платформа видеоконференцсвязи LiveDigital				
--	--	--	--	--	--	--

9. Методические материалы, определяющие процедуры оценивания результатов обучения

Оценочные процедуры и их краткое описание.

Итоговой формой аттестации по дисциплине является - **экзамен**.

Процедура оценивания результатов успеваемости студентов по дисциплине предполагает проведение текущей, рубежной и промежуточной аттестации. Материалы оценочных средств представлены в фонде оценочных средств учебной дисциплины дисциплине (см. приложение ФОС по дисциплине)

Виды контроля	Оценочное средство
Текущий контроль	тестирование, практико-ориентированные задания, доклад, реферат, эссе
Рубежный контроль	контрольная работа (тесты, задания)
Промежуточный контроль	тестирование, практико-ориентированные задания

9.1. Описание оценочных средств текущего, рубежного и промежуточного контроля

№	Наименование ОС (процесс / конечный продукт)	Краткая характеристика оценочного средства	Контрольно-измерительные материалы
1	Опрос	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Тестовые задания, вопросы по темам, разделам, практико-ориентированные задания
2	Тестирование	Система стандартизированных простых и комплексных заданий, позволяющая автоматизировать процедуру измерения уровня знаний, умений и владений обучающегося. Рекомендуется для оценки знаний, умений и владений студентов.	Тестовые задания
3	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу, выполняется в письменном виде по предложенным вопросам	Тестовые задания, вопросы по темам, разделам, практико-ориентированные задания
4	Практические задания и кейсы	Частично регламентированное задание по практической подготовке в профессиональной деятельности, имеющее алгоритмическое или нестандартное решение, позволяющее диагностировать умения, интегрировать знания различных научных областей в практическую подготовку, связанную с профессиональной деятельностью. Может выполняться в индивидуальном порядке или группой обучающихся.	практико-ориентированные задания
5	Доклад	Расширенное письменное или устное сообщение на основе совокупности ранее опубликованных исследовательских, научных разработок, по соответствующей отрасли научных знаний, имеющих значение для теории науки и практического применения. Представляет собой обобщенное изложение результатов проведенных исследований, экспериментов и разработок, известных широкому кругу специалистов в отрасли научных знаний.	темы докладов; критерии оценки
6	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной учебно-исследовательской темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	темы рефератов; критерии оценки
7	Эссе	Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Выполняется индивидуально в письменной форме по выбранной теме.	темы эссе; критерии оценки

9.2. Формы текущего/рубежного контроля успеваемости и достижения результатов обучения

№	Наименование и содержание по темам (разделам)	Краткое содержание	Формы текущего контроля	Компетенции
1	Тема 1. Понятие и основы информационной безопасности	Информация как объект защиты, свойства конфиденциальности, целостности и доступности, понятие угрозы и защиты информации. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
2	Тема 2. Нормативно-правовая база информационной безопасности в Российской Федерации	Система нормативных актов в области защиты информации: Конституция, 149-ФЗ, 152-ФЗ, 187-ФЗ, приказы ФСТЭК и ФСБ России. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
3	Тема 3. Федеральный закон № 152-ФЗ «О персональных данных»	Основные понятия закона, принципы и условия обработки персональных данных, права субъекта персональных данных. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
4	Тема 4. Категории персональных данных	Общие, специальные и биометрические персональные данные, особенности обработки сведений о состоянии здоровья. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
5	Тема 5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья	Правовой режим врачебной тайны, сведения о психическом здоровье, конфиденциальность в цифровых сервисах психологической помощи. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
6	Тема 6. Оператор персональных данных: обязанности и ответственность	Обязанности оператора, уведомление Роскомнадзора, ответственность за нарушение законодательства о персональных данных. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
7	Тема 7. Согласие на обработку персональных данных	Формы и содержание согласия, согласие на обработку специальных категорий, отзыв согласия субъектом. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
8	Тема 8. Трансграничная передача персональных данных	Условия трансграничной передачи, адекватность защиты, локализация баз данных на территории Российской Федерации. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
9	Тема 9. Угрозы информационной безопасности и модель нарушителя	Классификация угроз, источники угроз, построение модели угроз и модели нарушителя. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты	Опрос. Тестирование	УК-8, ОПК-3

		информации.		
10	Тема 10. Уязвимости и атаки на информационные системы	Понятие уязвимости, классификация атак, банк данных угроз безопасности информации ФСТЭК России. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
11	Тема 11. Вредоносное программное обеспечение	Виды вредоносного программного обеспечения, механизмы заражения и распространения, средства антивирусной защиты. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
12	Тема 12. Социальная инженерия и фишинг	Методы социальной инженерии, фишинг и его разновидности, меры противодействия и обучение пользователей. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
13	Тема 13. Криптографические методы защиты информации	Симметричное и асимметричное шифрование, хеш-функции, российские криптографические стандарты. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
14	Тема 14. Электронная подпись и удостоверяющие центры	Виды электронной подписи по 63-ФЗ, инфраструктура удостоверяющих центров, проверка подлинности подписи. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
15	Тема 15. Идентификация, аутентификация и управление доступом	Модели управления доступом, многофакторная аутентификация, разграничение прав в информационных системах. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
16	Тема 16. Межсетевые экраны и системы обнаружения вторжений	Функции межсетевых экранов, системы обнаружения и предотвращения вторжений, сегментация сети. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
17	Тема 17. Защита информации в компьютерных сетях	Защищенные сетевые протоколы, виртуальные частные сети, протокол TLS, безопасность передачи данных. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
18	Тема 18. Безопасность веб-приложений и мобильных сервисов	Типовые уязвимости веб-приложений, защита программных интерфейсов, безопасность мобильных приложений сервисов ментального здоровья. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
19	Тема 19. Категорирование информационных систем персональных данных	Порядок отнесения информационных систем персональных данных к категориям, определение типа актуальных угроз, обследование систем. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами за-	Опрос. Тестирование	УК-8, ОПК-3

		щиты информации.		
20	Тема 20. Определение уровней защищенности информационных систем персональных данных	Уровни защищенности по постановлению Правительства № 1119, состав мер защиты для каждого уровня. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
21	Тема 21. Средства защиты информации и их сертификация	Классы средств защиты информации, сертификация ФСТЭК и ФСБ России, применение сертифицированных средств. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
22	Тема 22. Организационные меры защиты информации	Политика информационной безопасности, регламенты, разграничение ответственности, режим служебной тайны. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
23	Тема 23. Управление инцидентами информационной безопасности	Выявление, регистрация и реагирование на инциденты, взаимодействие с ГосСОПКА, расследование инцидентов. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
24	Тема 24. Резервное копирование и восстановление данных	Стратегии резервного копирования, планы обеспечения непрерывности и восстановления, тестирование резервных копий. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
25	Тема 25. Аудит информационной безопасности	Внутренний и внешний аудит, оценка соответствия требованиям, тестирование на проникновение. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3
26	Тема 26. Обеспечение безопасности сервисов ментального здоровья: комплексный подход	Проектирование системы защиты цифрового сервиса психологической помощи, защита персональных данных и врачебной тайны, комплекс организационных и технических мер. Рассматриваются определения, требования, методы решения типовых задач и способы проверки результата. Показаны связи темы с задачами защиты информации.	Опрос. Тестирование	УК-8, ОПК-3

9.3. Критерии оценки результатов текущего и рубежного контроля

Критерии оценки	Баллы	Оценка
Опрос		
обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения	5	Отлично

компетенций(-ями); обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенций(-ями);	4	Хорошо
обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенций(-ями);	3	Удовлетворительно
обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенций(-ями).	2	Неудовлетворительно
Тестирование		
Количество выполненных тестовых заданий		
90-100%	5	Отлично
74-89%	4	Хорошо
60-73%	3	Удовлетворительно
менее 60%	2	Неудовлетворительно
Контрольная работа		
показан высокий уровень знания изученного материала по заданной теме, проявлен творческий подход при ответе на вопросы, умение глубоко анализировать проблему и делать обобщающие выводы; – работа выполнена грамотно с точки зрения поставленной задачи, т.е. без ошибок и недочетов или допущено не более одного недочета	5	Отлично
показан достаточный уровень знания изученного материала по заданной теме, проявлен творческий подход при ответе на вопросы, умение анализировать проблему и делать обобщающие выводы; – работа выполнена полностью, но допущено в ней: а) не более одной негрубой ошибки и одного недочета б) или не более двух недочетов.	4	Хорошо
показаны минимальные знания по основным темам контрольной работы; – выполнено не менее половины работы или допущены в ней: а) не более двух грубых ошибок, б) не более одной грубой ошибки и одного недочета, в) не более двух-трех негрубых ошибок, г) одна негрубая ошибка и три недочета, д) при отсутствии ошибок, 4-5 недочетов	3	Удовлетворительно
число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «удовлетворительно» или если правильно выполнено менее половины работы; – если обучающийся не приступал к выполнению работы или правильно выполнил не более 10 процентов всех заданий	2	Неудовлетворительно
Практические задания, кейсы		
продемонстрировано грамотное последовательное решение задач (заданий) при правильно выбранном алгоритме. Даны верные ответы на все вопросы и условия задач (заданий). При необходимости сделаны пояснения и выводы (содержательные, достаточно полные, правильные, учитывающие специфику проблемной ситуации в задаче или с незначительными ошибками);	5	Отлично
грамотное последовательное решение задач (заданий) при правильно выбранном алгоритме. Однако, ответы на вопросы и условия задач (заданий) содержат незначительные ошибки. По-	4	Хорошо

яснения и выводы отсутствуют или даны неверно		
обучающийся ориентируется в материале, но применяет его неверно, выбирает неправильный алгоритм решения задач (неверные исходные данные, неверная последовательность решения и др. ошибки), допускает ошибки. Пояснения и выводы отсутствуют или даны неверно	3	Удовлетворительно
обучающийся слабо ориентируется в материале, выбирает неправильный алгоритм решения, допускает значительное количество вычислительных ошибок. Пояснения и выводы отсутствуют	2	Неудовлетворительно
Доклад, реферат, эссе		
Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, заявленная тема полностью раскрыта, рассмотрение дискуссионных вопросов по проблеме, сопоставлены различные точки зрения по рассматриваемому вопросу, научность языка изложения, логичность и последовательность в изложении материала, количество исследованной литературы, в том числе новейших источников по проблеме, четкость выводов, оформление работы соответствует предъявляемым требованиям.	5	Отлично
Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, научность языка изложения, заявленная тема раскрыта недостаточно полно, отсутствуют новейшие литературные источники по проблеме, при оформлении работы имеются недочеты.	4	Хорошо
Соответствие целям и задачам дисциплины, содержание работы не в полной мере соответствует заявленной теме, заявленная тема раскрыта недостаточно полно, использовано небольшое количество научных источников, нарушена логичность и последовательность в изложении материала, при оформлении работы имеются недочеты	3	Удовлетворительно
Работа не соответствует целям и задачам дисциплины, содержание работы не соответствует заявленной теме, содержание работы изложено не научным стилем	2	Неудовлетворительно

9.4. Процедура промежуточной аттестации

Процедура промежуточной аттестации с дополнительным аттестационным испытанием (Экзамен)

Сдача экзамена предусмотрена в форме выполнения тестовых и практико-ориентированных заданий по дисциплине (см. ФОС). Продолжительность тестирования - 30 минут.

При проведении компьютерного тестирования оценка результатов определяется по сумме баллов, полученных за правильно выполненные тестовые оценочные задания.

Оценка «отлично» выставляется, если обучающимся набрано от 85 до 100 баллов;

оценка «хорошо» - от 67 до 84 баллов;

оценка «удовлетворительно» - от 50 до 66 баллов;

оценка «неудовлетворительно» - 49 баллов и менее.

Оценивание обучающегося на промежуточной аттестации в форме экзамена осуществляется в соответствии с критериями, представленными в таблице, и носит балльный характер.

9.5. Критерии оценки образовательных результатов обучающихся на экзамене по дисциплине:

Результат экзамена	Критерии оценки образовательных результатов
--------------------	---

5, отлично	Оценка «5 (отлично)» выставляется обучающемуся, если по результатам выполнения экзаменационных заданий им набрано от 85 до 100 баллов. При этом обучающийся при выполнении тестовых и практико-ориентированных заданий экзамена продемонстрировал глубокое и прочное усвоение программного материала, умение тесно увязывать теорию с практикой, свободно справлялся с заданиями и вопросами, не затруднялся с ответом при видоизменении заданий, правильно обосновывал принятые решения. Компетенции, закрепленные за дисциплиной, сформированы на уровне - высокий.
4, хорошо	Оценка «4 (хорошо)» выставляется обучающемуся, если по результатам выполнения экзаменационных заданий им набрано от 67 до 84 баллов. При этом обучающийся при выполнении тестовых и практико-ориентированных заданий экзамена продемонстрировал твердое знание программного материала, грамотно и по существу отвечал на вопросы, не допускал существенных неточностей, правильно применял теоретические положения при решении практико-ориентированных заданий. Компетенции, закрепленные за дисциплиной, сформированы на уровне - хороший (средний).
3, удовлетворительно	Оценка «3 (удовлетворительно)» выставляется обучающемуся, если по результатам выполнения экзаменационных заданий им набрано от 50 до 66 баллов. При этом обучающийся при выполнении тестовых и практико-ориентированных заданий экзамена продемонстрировал знание только основного программного материала без усвоения его деталей, допускал неточности и недостаточно правильные формулировки, испытывал затруднения при выполнении практико-ориентированных заданий. Компетенции, закрепленные за дисциплиной, сформированы на уровне - достаточный.
2, неудовлетворительно	Оценка «2 (неудовлетворительно)» выставляется обучающемуся, если по результатам выполнения экзаменационных заданий им набрано 49 баллов и менее. При этом обучающийся при выполнении тестовых и практико-ориентированных заданий экзамена продемонстрировал незнание значительной части программного материала, допускал существенные ошибки, не справлялся с практико-ориентированными заданиями. Как правило, оценка «неудовлетворительно» выставляется обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Компетенции, закрепленные за дисциплиной, сформированы на недостаточном уровне или не сформированы.

9.6. Соответствие уровня освоения компетенции планируемым результатам обучения и критериям их оценивания

Код	Содержание компетенции
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Показатель оценивания/результаты обучения	Критерии оценивания			
	2 (неудовлетворительно)	3 (удовлетворительно)	4 (хорошо)	5 (отлично)
Знает (УК-8)	Не знает: основы безопасности жизнедеятельности и охраны окружающей среды; требования законодательства Российской Федерации в области гражданской обороны и защиты от чрез-	Демонстрирует только частичное знание: основы безопасности жизнедеятельности и охраны окружающей среды; требования законодательства Российской	Демонстрирует знание: основы безопасности жизнедеятельности и охраны окружающей среды; требования законодательства Российской Федерации в	Знает в полной мере: основы безопасности жизнедеятельности и охраны окружающей среды; требования законодательства Российской Федерации в

	выдающихся ситуаций; принципы устойчивого развития; правила оказания первой помощи	ской Федерации в области гражданской обороны и защиты от чрезвычайных ситуаций; принципы устойчивого развития; правила оказания первой помощи	области гражданской обороны и защиты от чрезвычайных ситуаций; принципы устойчивого развития; правила оказания первой помощи	области гражданской обороны и защиты от чрезвычайных ситуаций; принципы устойчивого развития; правила оказания первой помощи
Умеет (УК-8)	Не умеет: идентифицировать опасные и вредные факторы в быту и профессиональной среде; применять средства индивидуальной и коллективной защиты; действовать в условиях чрезвычайных ситуаций; оказывать первую помощь	Демонстрирует только частичное умение: идентифицировать опасные и вредные факторы в быту и профессиональной среде; применять средства индивидуальной и коллективной защиты; действовать в условиях чрезвычайных ситуаций; оказывать первую помощь	Демонстрирует умение: идентифицировать опасные и вредные факторы в быту и профессиональной среде; применять средства индивидуальной и коллективной защиты; действовать в условиях чрезвычайных ситуаций; оказывать первую помощь	Умеет в полной мере: идентифицировать опасные и вредные факторы в быту и профессиональной среде; применять средства индивидуальной и коллективной защиты; действовать в условиях чрезвычайных ситуаций; оказывать первую помощь
Владеет (УК-8)	Не владеет: навыками обеспечения безопасности в быту и профессиональной деятельности; приемами поведения при чрезвычайных ситуациях и военных конфликтах; методами минимизации негативного воздействия на природную среду	Демонстрирует только частичное владение: навыками обеспечения безопасности в быту и профессиональной деятельности; приемами поведения при чрезвычайных ситуациях и военных конфликтах; методами минимизации негативного воздействия на природную среду	Демонстрирует владение: навыками обеспечения безопасности в быту и профессиональной деятельности; приемами поведения при чрезвычайных ситуациях и военных конфликтах; методами минимизации негативного воздействия на природную среду	Владеет в полной мере: навыками обеспечения безопасности в быту и профессиональной деятельности; приемами поведения при чрезвычайных ситуациях и военных конфликтах; методами минимизации негативного воздействия на природную среду
Знает (ОПК-3)	Не знает: основы информационной и библиографической культуры; состав профессиональных информационных ресурсов в сфере информационных технологий; требования Федерального закона № 152-ФЗ «О персональных данных» и основ информационной безопасности	Демонстрирует только частичное знание: основы информационной и библиографической культуры; состав профессиональных информационных ресурсов в сфере информационных технологий; требования Федерального закона № 152-ФЗ «О персональных данных» и основ информационной безопасности	Демонстрирует знание: основы информационной и библиографической культуры; состав профессиональных информационных ресурсов в сфере информационных технологий; требования Федерального закона № 152-ФЗ «О персональных данных» и основ информационной безопасности	Знает в полной мере: основы информационной и библиографической культуры; состав профессиональных информационных ресурсов в сфере информационных технологий; требования Федерального закона № 152-ФЗ «О персональных данных» и основ информационной безопасности
Умеет (ОПК-3)	Не умеет: пользоваться ИКТ и профессиональными информационными ресурсами при реше-	Демонстрирует только частичное умение: пользоваться ИКТ и профессиональными	Демонстрирует умение: пользоваться ИКТ и профессиональными	Умеет в полной мере: пользоваться ИКТ и профессиональными

	нии стандартных задач; оформлять библиографические ссылки и списки литературы; применять базовые меры по защите информации	информационными ресурсами при решении стандартных задач; оформлять библиографические ссылки и списки литературы; применять базовые меры по защите информации	ми ресурсами при решении стандартных задач; оформлять библиографические ссылки и списки литературы; применять базовые меры по защите информации	сурсами при решении стандартных задач; оформлять библиографические ссылки и списки литературы; применять базовые меры по защите информации
Владеет (ОПК-3)	Не владеет: навыками работы с профессиональной информацией с учетом требований информационной безопасности; приемами защиты персональных данных и обеспечения конфиденциальности в информационных системах	Демонстрирует только частичное владение: навыками работы с профессиональной информацией с учетом требований информационной безопасности; приемами защиты персональных данных и обеспечения конфиденциальности в информационных системах	Демонстрирует владение: навыками работы с профессиональной информацией с учетом требований информационной безопасности; приемами защиты персональных данных и обеспечения конфиденциальности в информационных системах	Владеет в полной мере: навыками работы с профессиональной информацией с учетом требований информационной безопасности; приемами защиты персональных данных и обеспечения конфиденциальности в информационных системах

10. Оценочные средства для проведения контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины и основной профессиональной образовательной программы.

Фонд оценочных средств представляет собой комплекс учебных заданий, предназначенных для измерения уровня достижений обучающимся установленных результатов обучения, и используется при проведении текущей и промежуточной аттестации (в период зачетно-экзаменационной сессии).

Цель ФОС - установление соответствия уровня подготовки обучающихся на данном этапе обучения требованиям рабочей программы дисциплины.

Основными задачами ФОС по учебной дисциплине являются:

- контроль достижений целей реализации ОП - формирование компетенций;
- контроль процесса приобретения обучающимся необходимых знаний, умений, навыков (владения/опыта деятельности) и уровня сформированности компетенций;
- оценка достижений обучающегося;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование методов обучения в образовательном процессе.

10.1. Типовые контрольные задания для проведения текущей/рубежной аттестации по дисциплине (модулю).

Примерный перечень тем (доклад, реферат, эссе)

Примерные темы докладов.

1. Понятие и основы информационной безопасности: содержание, нормативные требования и область применения.
2. Нормативно-правовая база информационной безопасности в Российской Федерации: содержание, нормативные требования и область применения.
3. Федеральный закон № 152-ФЗ «О персональных данных»: содержание, нормативные требования и область применения.
4. Категории персональных данных: содержание, нормативные требования и область применения.
5. Врачебная тайна и конфиденциальность в сервисах ментального здоровья: содержание, нормативные требования и область применения.
6. Оператор персональных данных: обязанности и ответственность: содержание, нормативные требования и область применения.
7. Согласие на обработку персональных данных: содержание, нормативные требования и область применения.
8. Трансграничная передача персональных данных: содержание, нормативные требования и область применения.
9. Угрозы информационной безопасности и модель нарушителя: содержание, нормативные требования и область применения.
10. Уязвимости и атаки на информационные системы: содержание, нормативные требования и область применения.

Примерные темы рефератов.

1. Сравнительный анализ подходов по теме «Вредоносное программное обеспечение».
2. Сравнительный анализ подходов по теме «Социальная инженерия и фишинг».
3. Сравнительный анализ подходов по теме «Криптографические методы защиты информации».
4. Сравнительный анализ подходов по теме «Электронная подпись и удостоверяющие центры».
5. Сравнительный анализ подходов по теме «Идентификация, аутентификация и управление доступом».

6. Сравнительный анализ подходов по теме «Межсетевые экраны и системы обнаружения вторжений».
7. Сравнительный анализ подходов по теме «Защита информации в компьютерных сетях».
8. Сравнительный анализ подходов по теме «Безопасность веб-приложений и мобильных сервисов».
9. Сравнительный анализ подходов по теме «Категорирование информационных систем персональных данных».
10. Сравнительный анализ подходов по теме «Определение уровней защищенности информационных систем персональных данных».

Примерные темы эссе.

1. Роль дисциплины «Информационная безопасность» в защите персональных данных и врачебной тайны в сервисах ментального здоровья.
2. Почему обеспечение информационной безопасности требует сочетания организационных и технических мер.
3. Как категорирование информационной системы влияет на выбор мер защиты.
4. Почему защита сведений о психическом здоровье имеет особый правовой режим.
5. Как соблюдение требований 152-ФЗ влияет на доверие пользователей цифрового сервиса.

Типовые контрольные задания для проведения рубежного контроля по дисциплине (модулю).

Контрольная работа № 1

Вариант 1

1. Раскройте принципы и условия обработки персональных данных по теме «Федеральный закон № 152-ФЗ «О персональных данных»».
2. Опишите порядок построения модели угроз по теме «Угрозы информационной безопасности и модель нарушителя».

Вариант 2

1. Определите состав мер защиты по теме «Определение уровней защищенности информационных систем персональных данных».
2. Обоснуйте выбор средств защиты по теме «Средства защиты информации и их сертификация».

Контрольная работа № 2

Вариант 1

1. Разработайте перечень организационных мер по теме «Организационные меры защиты информации».
2. Опишите порядок реагирования по теме «Управление инцидентами информационной безопасности».

Вариант 2

1. Предложите схему защиты каналов по теме «Защита информации в компьютерных сетях».
2. Составьте план обеспечения безопасности по теме «Обеспечение безопасности сервисов ментального здоровья: комплексный подход».

10.2. Примерный перечень тестовых заданий для текущего/рубежного/промежуточного контроля

Система оценивания тестовых заданий

Типы заданий	Время выполнения заданий (мин.)	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задание закрытого типа с выбором одного верного ответа	2	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задание закрытого типа с выбором 2 вариантов ответа	3	Полное совпадение с верным ответом оценивается 2 баллами; если допущена 1 ошибка - 1 балл; более 1 ошибки или ответ отсутствует - 0 баллов.
Задание открытого типа на дополнение	4	Полный правильный ответ на задание оценивается 2 баллами; если допущены ошибки или ответ отсутствует - 0 баллов.
Задание закрытого типа на установление соответствия	6	Полное совпадение с верным ответом оценивается 3 баллами; если допущена 1 ошибка - 2 балла, если допущены 2 ошибки - 1 балл, если допущены более 2 ошибок или ответ отсутствует - 0 баллов.
Задание закрытого типа (практико-ориентированные задания, кейсы)	5	Совпадение с верным ответом оценивается 5 баллами; неверный ответ или его отсутствие - 0 баллов.

Примерные тестовые задания

П/Н	Номер задания	Правильный ответ	Содержание вопроса
		Задания с 1 вариантом ответа	
1.	УК-8.1.1	персональные данные	Какое понятие соответствует определению: любая информация, относящаяся к прямо или косвенно определенному физическому лицу? 1) персональные данные 2) обезличивание 3) аутентификация 4) удостоверяющий центр
2.	УК-	конфиденциальность ин-	Какое понятие соответствует определению: свойство

	8.2.2	формации	информации быть недоступной неавторизованным лицам? 1) целостность информации 2) доступность информации 3) конфиденциальность информации 4) категорирование
3.	УК-8.3.3	целостность информации	Какое понятие соответствует определению: свойство информации сохранять неизменность и полноту? 1) доступность информации 2) целостность информации 3) конфиденциальность информации 4) обезличивание
4.	ОПК-3.1.4	доступность информации	Какое понятие соответствует определению: свойство информации быть предоставленной авторизованным пользователям по запросу? 1) целостность информации 2) доступность информации 3) шифрование 4) инцидент безопасности
5.	ОПК-3.2.5	врачебная тайна	Какое понятие соответствует определению: охраняемые законом сведения о факте обращения за медицинской помощью, диагнозе и состоянии здоровья? 1) врачебная тайна 2) коммерческая тайна 3) банковская тайна 4) обезличивание
6.	ОПК-3.3.6	оператор персональных данных	Какое понятие соответствует определению: лицо, организующее и осуществляющее обработку персональных данных? 1) оператор персональных данных 2) субъект персональных данных 3) удостоверяющий центр 4) средство защиты информации
7.	ОПК-3.1.7	модель угроз	Какое понятие соответствует определению: документ, описывающий актуальные угрозы безопасности информации конкретной системы? 1) политика безопасности 2) модель угроз 3) согласие субъекта 4) электронная подпись
8.	УК-8.2.8	шифрование	Какое понятие соответствует определению: криптографическое преобразование информации для защиты ее конфиденциальности? 1) аутентификация 2) категорирование 3) резервное копирование 4) шифрование
9.	ОПК-3.3.9	электронная подпись	Какое понятие соответствует определению: реквизит электронного документа, позволяющий установить подписанта и неизменность документа? 1) межсетевой экран 2) модель нарушителя 3) обезличивание 4) электронная подпись
10.	УК-8.1.10	межсетевой экран	Какое понятие соответствует определению: средство контроля и фильтрации сетевого трафика между сетями с разными требованиями безопасности? 1) межсетевой экран 2) удостоверяющий центр 3) согласие субъекта 4) врачебная тайна
Задания с 2 вариантами ответа			

11.	УК-8.1.1	относятся к определенному или определяемому физическому лицу; могут относиться к специальным категориям	Выберите два верных утверждения о понятии «персональные данные»: 1) утрачивают статус персональных данных после размещения в сети Интернет 2) включают только сведения, позволяющие установить личность без дополнительной информации 3) относятся к определенному или определяемому физическому лицу 4) относятся как к физическим, так и к юридическим лицам 5) могут относиться к специальным категориям
12.	УК-8.2.2	должно быть конкретным, информированным и сознательным; может быть отозвано субъектом персональных данных	Выберите два верных утверждения о понятии «согласие на обработку персональных данных»: 1) должно быть конкретным, информированным и сознательным 2) в отношении сведений о здоровье может выражаться конклюдентными действиями пользователя 3) действует бессрочно и не может ограничиваться сроком 4) может быть отозвано субъектом персональных данных 5) во всех случаях оформляется только в письменной форме
13.	УК-8.3.3	включают сведения о состоянии здоровья; обрабатываются при наличии установленных законом условий	Выберите два верных утверждения о понятии «специальные категории персональных данных»: 1) включают биометрические персональные данные 2) включают сведения о состоянии здоровья 3) включают сведения о семейном и имущественном положении 4) обрабатываются при наличии установленных законом условий 5) могут обрабатываться при наличии согласия субъекта в устной форме
14.	ОПК-3.1.4	обязан обеспечивать защиту обрабатываемых данных; несет ответственность за нарушение требований закона	Выберите два верных утверждения о понятии «оператор персональных данных»: 1) освобождается от ответственности перед субъектом, поручив обработку другому лицу 2) обязан получить разрешение Роскомнадзора до начала обработки 3) может быть только юридическим лицом 4) обязан обеспечивать защиту обрабатываемых данных 5) несет ответственность за нарушение требований закона
15.	ОПК-3.2.5	охраняется законом; включает сведения о психическом состоянии пациента	Выберите два верных утверждения о понятии «врачебная тайна»: 1) охраняется законом 2) прекращает действие после смерти пациента 3) не распространяется на сведения о факте обращения за медицинской помощью 4) может раскрываться работодателю пациента по его запросу без согласия пациента 5) включает сведения о психическом состоянии пациента
16.	ОПК-3.3.6	обеспечивает защиту конфиденциальности информации; бывает симметричным и асимметричным	Выберите два верных утверждения о понятии «шифрование»: 1) является необратимым преобразованием информации 2) в асимметричной схеме использует один общий секретный ключ 3) обеспечивает защиту конфиденциальности информации 4) обеспечивает сохранность данных при отказе но-

			сителя 5) бывает симметричным и асимметричным
17.	УК-8.1.7	позволяет установить подписанта документа; подтверждает неизменность подписанного документа	Выберите два верных утверждения о понятии «электронная подпись»: 1) позволяет установить подписанта документа 2) обеспечивает конфиденциальность содержания подписанного документа 3) подтверждает неизменность подписанного документа 4) создается с использованием ключа проверки электронной подписи 5) в виде простой электронной подписи во всех случаях равнозначна собственноручной
18.	ОПК-3.2.8	использует несколько независимых факторов подтверждения; повышает защищенность доступа	Выберите два верных утверждения о понятии «многофакторная аутентификация»: 1) обеспечивается вводом двух разных паролей подряд 2) заменяет разграничение прав доступа пользователей 3) использует несколько независимых факторов подтверждения 4) повышает защищенность доступа 5) полностью исключает успешные фишинговые атаки на пользователей
19.	УК-8.3.9	определяется с учетом типа актуальных угроз; влияет на состав применяемых мер защиты	Выберите два верных утверждения о понятии «уровень защищенности информационной системы персональных данных»: 1) определяется с учетом типа актуальных угроз 2) определяется ФСТЭК России для каждой системы оператора 3) имеет четыре значения, из которых 4-й уровень - наивысший 4) определяется по числу сотрудников оператора, имеющих доступ к системе 5) влияет на состав применяемых мер защиты
20.	УК-8.1.10	подлежит выявлению и регистрации; требует реагирования и расследования	Выберите два верных утверждения о понятии «инцидент информационной безопасности»: 1) является синонимом понятия «угроза информационной безопасности» 2) подлежит выявлению и регистрации 3) расследуется только правоохранительными органами 4) требует реагирования и расследования 5) касается только внешних атак на систему
Задания открытого типа на дополнение			
21.	УК-8.1.1	обезличивание персональных данных	Укажите термин: действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту без дополнительной информации.
22.	УК-8.2.2	аутентификация	Укажите термин: проверка подлинности предъявленного субъектом доступа идентификатора.
23.	УК-8.3.3	идентификация	Укажите термин: присвоение субъектам и объектам доступа уникального признака и его сравнение с перечнем присвоенных.
24.	ОПК-3.1.4	уязвимость	Укажите термин: недостаток информационной системы, использование которого нарушителем может привести к реализации угрозы.
25.	ОПК-3.2.5	категорирование информационной системы персональных данных	Укажите термин: отнесение информационной системы к определенной категории с учетом объема и характера обрабатываемых данных.
26.	ОПК-3.3.6	локализация персональных данных	Укажите термин: обязанность обеспечивать запись, систематизацию и хранение персональных данных

			граждан России с использованием баз данных на территории Российской Федерации.
27.	ОПК-3.1.7	удостоверяющий центр	Укажите термин: организация, осуществляющая создание и выдачу сертификатов ключей проверки электронной подписи.
28.	УК-8.2.8	средство защиты информации	Укажите термин: техническое, программное или программно-техническое средство, предназначенное для защиты информации.
29.	ОПК-3.3.9	политика информационной безопасности	Укажите термин: документ, определяющий цели, принципы и правила обеспечения защиты информации в организации.
30.	УК-8.1.10	модель нарушителя	Укажите термин: описание предполагаемых возможностей, мотивации и категорий нарушителей безопасности информации.
Задания на установление соответствия			
31.	УК-8.1.1	1 - конфиденциальность; 2 - целостность; 3 - доступность; 4 - аутентичность	Установите соответствие между свойством информации и его определением: 1) недоступность неавторизованным лицам 2) неизменность и полнота 3) предоставление авторизованным пользователям по запросу 4) идентичность субъекта или ресурса заявленному а) целостность б) аутентичность в) конфиденциальность г) доступность
32.	УК-8.2.2	1 - 152-ФЗ; 2 - 63-ФЗ; 3 - 187-ФЗ; 4 - 149-ФЗ	Установите соответствие между сферой регулирования и федеральным законом: 1) обработка персональных данных 2) электронная подпись 3) безопасность критической информационной инфраструктуры 4) общие правовые основы в сфере информации, информационных технологий и защиты информации а) 149-ФЗ б) 187-ФЗ в) 152-ФЗ г) 63-ФЗ
33.	УК-8.3.3	1 - оператор; 2 - субъект персональных данных; 3 - уполномоченный орган по защите прав субъектов; 4 - лицо, осуществляющее обработку по поручению оператора	Установите соответствие между ролью и ее описанием: 1) организует обработку данных 2) физическое лицо, к которому относятся данные 3) осуществляет надзор за обработкой данных 4) обрабатывает данные на основании договора с оператором а) уполномоченный орган по защите прав субъектов б) лицо, осуществляющее обработку по поручению оператора в) субъект персональных данных г) оператор
34.	ОПК-3.1.4	1 - симметричное шифрование; 2 - асимметричное шифрование; 3 - хеширование; 4 - гибридное шифрование	Установите соответствие между криптографическим методом и признаком: 1) один общий ключ для шифрования и расшифрования 2) пара из открытого и закрытого ключей 3) необратимое преобразование фиксированной длины 4) шифрование данных сеансовым ключом с передачей этого ключа под защитой открытого ключа полу-

			чателя а) хеширование б) симметричное шифрование в) гибридное шифрование г) асимметричное шифрование
35.	ОПК-3.2.5	1 - фишинг; 2 - вредоносное ПО; 3 - отказ в обслуживании; 4 - атака «человек посередине»	Установите соответствие между угрозой и ее проявлением: 1) обманное получение учетных данных пользователя 2) заражение системы вредоносным кодом 3) исчерпание ресурсов и недоступность сервиса 4) скрытый перехват и подмена трафика в канале связи между сторонами а) атака «человек посередине» б) отказ в обслуживании в) фишинг г) вредоносное ПО
36.	ОПК-3.3.6	1 - межсетевой экран; 2 - система обнаружения вторжений; 3 - антивирус; 4 - виртуальная частная сеть	Установите соответствие между средством защиты и его функцией: 1) фильтрация сетевого трафика 2) выявление признаков атак 3) обнаружение и удаление вредоносного ПО 4) построение зашифрованного туннеля между удаленными узлами через интернет а) антивирус б) межсетевой экран в) виртуальная частная сеть г) система обнаружения вторжений
37.	УК-8.1.7	1 - идентификация; 2 - аутентификация; 3 - авторизация; 4 - протоколирование	Установите соответствие между этапом доступа и его содержанием: 1) предъявление идентификатора 2) проверка подлинности идентификатора 3) предоставление прав доступа 4) фиксация действий пользователя в журнале событий а) аутентификация б) протоколирование в) идентификация г) авторизация
38.	ОПК-3.2.8	1 - согласие; 2 - модель угроз; 3 - политика безопасности; 4 - уведомление	Установите соответствие между документом и его назначением: 1) разрешение субъекта на обработку данных 2) описание актуальных угроз системы 3) правила обеспечения защиты информации в организации 4) сообщение оператора в уполномоченный орган о намерении обрабатывать данные а) уведомление б) политика безопасности в) согласие г) модель угроз
39.	УК-8.3.9	1 - УЗ-1; 2 - УЗ-2; 3 - УЗ-3; 4 - УЗ-4	Установите соответствие между условиями обработки персональных данных в информационной системе и уровнем защищенности по требованиям, утвержденным постановлением Правительства РФ от 01.11.2012 № 1119: 1) актуальны угрозы 1-го типа, обрабатываются специальные категории персональных данных 2) актуальны угрозы 2-го типа, обрабатываются био-

			метрические персональные данные 3) актуальны угрозы 3-го типа, обрабатываются биометрические персональные данные 4) актуальны угрозы 3-го типа, обрабатываются общедоступные персональные данные а) УЗ-3 б) УЗ-1 в) УЗ-4 г) УЗ-2
40.	УК-8.1.10	1 - резервное копирование; 2 - аудит безопасности; 3 - управление инцидентами; 4 - обучение пользователей	Установите соответствие между мерой и целью: 1) восстановление данных после сбоя 2) оценка соответствия требованиям 3) реагирование на нарушения безопасности 4) снижение восприимчивости работников к приемам социальной инженерии а) управление инцидентами б) резервное копирование в) обучение пользователей г) аудит безопасности
Практико-ориентированные задания (кейсы)			
41.	УК-8.1.1	получить от пользователя отдельное согласие на обработку специальных категорий персональных данных	Кейс. Онлайн-сервис психологической помощи собирает сведения о психическом состоянии клиентов. Какое действие является обоснованным? 1) ограничиться размещением на сайте политики обработки персональных данных 2) направить в Роскомнадзор уведомление об обработке и собирать сведения без согласия клиентов 3) получить общее согласие на обработку персональных данных без указания сведений о состоянии здоровья 4) получить от пользователя отдельное согласие на обработку специальных категорий персональных данных
42.	УК-8.2.2	обеспечить хранение персональных данных граждан России в базах данных на территории Российской Федерации	Кейс. Сервис планирует использовать зарубежный облачный хостинг для базы клиентов. Какое действие является обоснованным? 1) обеспечить хранение персональных данных граждан России в базах данных на территории Российской Федерации 2) разместить базу у зарубежного провайдера, получив согласие клиентов на трансграничную передачу 3) зашифровать базу данных и разместить ее у зарубежного провайдера 4) разместить базу у зарубежного провайдера по договору поручения обработки персональных данных
43.	УК-8.3.3	построить модель угроз и определить актуальные угрозы для информационной системы	Кейс. Перед вводом сервиса в эксплуатацию требуется оценить угрозы безопасности. Какое действие является обоснованным? 1) ограничиться установкой антивирусного средства и межсетевого экрана 2) использовать модель угроз аналогичной системы другой организации без анализа своей системы 3) провести оценку угроз после ввода сервиса в эксплуатацию по итогам первых инцидентов 4) построить модель угроз и определить актуальные угрозы для информационной системы
44.	ОПК-3.1.4	определить уровень защищенности и применить соответствующий состав мер защиты	Кейс. Информационная система обрабатывает специальные категории персональных данных клиентов. Какое действие является обоснованным? 1) определить уровень защищенности и применить соответствующий состав мер защиты

			2) применить меры защиты, предусмотренные для 4-го уровня защищенности, как для общедоступных данных 3) подобрать меры защиты по перечню ФСТЭК России, не определяя уровень защищенности 4) ограничиться организационными мерами: приказом о допуске и инструкцией пользователей
45.	ОПК-3.2.5	применить сертифицированные средства защиты информации и криптографические средства	Кейс. Требуется защитить каналы передачи сведений о здоровье между клиентом и сервисом. Какое действие является обоснованным? 1) ограничиться парольной защитой учетных записей клиентов 2) шифровать только вложенные файлы, передавая текст сообщений в открытом виде 3) применить средства шифрования, выбранные по скорости работы, без оценки их соответствия требованиям 4) применить сертифицированные средства защиты информации и криптографические средства
46.	ОПК-3.3.6	настроить многофакторную аутентификацию и разграничение прав доступа специалистов	Кейс. К данным клиентов имеют доступ несколько психологов и администраторов сервиса. Какое действие является обоснованным? 1) ограничиться требованием сложных паролей и их сменой раз в 90 дней 2) разграничить права доступа, оставив администраторам одну общую учетную запись 3) настроить многофакторную аутентификацию, предоставив всем специалистам одинаковый полный доступ к данным 4) настроить многофакторную аутентификацию и разграничение прав доступа специалистов
47.	ОПК-3.1.7	зарегистрировать инцидент, локализовать его и провести расследование	Кейс. Обнаружена утечка части сведений о клиентах сервиса ментального здоровья. Какое действие является обоснованным? 1) зарегистрировать инцидент, локализовать его и провести расследование 2) сменить пароли администраторов и продолжить работу сервиса в обычном режиме 3) сразу восстановить систему из резервной копии, чтобы быстрее возобновить работу сервиса 4) отложить расследование до планового аудита безопасности
48.	УК-8.2.8	обезличить персональные данные перед использованием их для аналитики	Кейс. Команда планирует анализировать эксплуатационные данные для улучшения сервиса. Какое действие является обоснованным? 1) ограничить круг аналитиков приказом о допуске и передать им данные в исходном виде 2) удалить из выборки только фамилии клиентов, сохранив контакты и даты рождения 3) обезличить персональные данные перед использованием их для аналитики 4) обезличить данные после завершения анализа, перед передачей в архив
49.	ОПК-3.3.9	предоставить субъекту возможность отозвать согласие и прекратить обработку его данных	Кейс. Клиент сервиса обратился с требованием прекратить обработку его персональных данных. Какое действие является обоснованным? 1) продолжить обработку до окончания срока действия согласия, указанного при регистрации 2) предоставить субъекту возможность отозвать согласие и прекратить обработку его данных 3) потребовать от клиента письменного обоснования причин отзыва согласия 4) прекратить только рассылку сообщений, продол-

			жив хранение и анализ данных клиента
50.	УК-8.1.10	организовать регулярное резервное копирование и проверку восстановления данных	Кейс. Существует риск потери данных клиентов из-за сбоя оборудования сервиса. Какое действие является обоснованным? 1) настроить зеркалирование дисков (RAID 1) вместо резервного копирования 2) организовать регулярное резервное копирование и проверку восстановления данных 3) создавать резервные копии на том же сервере без проверки восстановления 4) создать резервную копию однократно при вводе сервиса в эксплуатацию