Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Северо-Кавказский федеральный университет»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

УТВЕРЖДАЮ

И.О. директора Пятигорского института
(филиал) СКФУ
В.А. Фурсов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине ОП. 05 Основы информационной безопасности
Специальность 09.02.11 Разработка и управление программным обеспечением
Форма обучения очная

Пятигорск

1. Паспорт фонда оценочных средств

1.1. Область применения

Фонд оценочных средств (далее - ФОС) предназначен для оценивания знаний, умений, уровня сформированности компетенций студентов, обучающихся по специальности 09.02.11 Разработка и управление программным обеспечением по дисциплине ОП.05 Основы информационной безопасности.

ФОС составлен на основе ФГОС и рабочей программы дисциплины.

Промежуточная аттестация по дисциплине предусмотрена в форме экзамена с выставлением отметки по системе «отлично, хорошо, удовлетворительно, неудовлетворительно».

1.2. Планируемые результаты освоения дисциплины

ФОС позволяет оценить знания, умения, сформированность общих и профессиональных компетенций в соответствии с требованиями ФГОС и рабочей программой дисциплины.

Планируемые результаты освоения (знания и умения) и перечень осваиваемых компетенций (общих и профессиональных) указываются в соответствии с ФГОС, ОП и рабочей программой учебной дисциплины.

умения:

У.1. распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать и выделять её составные части;

У.2. определять задачи для поиска информации, необходимые источники, планировать процесс поиска, структурировать и оформлять результаты;

У.3. шифровать данные и обеспечивать их конфиденциальность;

У.4. анализировать требования безопасности информационных систем;

У.5. разрабатывать и реализовывать меры безопасности, включая хэширование паролей, сессионные токены и двухфакторную аутентификацию.

знания:

З.1. актуальный профессиональный и социальный контекст, основные источники информации и ресурсы для решения задач;

З.2. номенклатуру информационных источников, приемы структурирования информации, современные средства информатизации;

З.3. принципы безопасности хранения данных и методы защиты баз данных от внешних угроз;

З.4. принципы криптографии и методов шифрования данных, стандарты и протоколы безопасности;

З.5. законодательство и стандарты безопасности;

З.6. отраслевую нормативную документацию, современный отечественный и зарубежный опыт в области ИБ;

З.7. принципы и методы обеспечения безопасности информационных систем, источники угроз и меры по их предотвращению.

общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности,

применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

профессиональные компетенции:

ПК 1.1. Проектировать базы данных.

ПК 1.4. Администрировать базы данных.

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 3.1. Собирать исходные данные для разработки проектной документации на информационную систему.

ПК 3.2. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.

ПК 3.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 3.5. Интегрировать информационную систему с существующими информационными системами заказчика.

ПК 3.7. Разрабатывать техническую документацию на эксплуатацию информационной системы.

1.3. Формы контроля и оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по (учебной) дисциплине, направленные на формирование общих и профессиональных компетенций.

Таблица 1 Контроль и оценка освоения (учебной) дисциплины по темам (разделам)

Элементы учебной дисциплины	Формы контроля и оценивания			
	Текущий контроль		Промежуточная аттестация	
	Методы оценки *(заполняется в соответствии с разделом 4 рабочей программы)*	Проверяемые ПК, ОК, У, З	Методы оценки	Проверяемые ПК, ОК, У, З
Раздел 1. Основы информационной безопасности			Указываются в соответствии с учебным планом	Указываются в соответствии с рабочей программой
Тема 1.1. Введение в информационную безопасность	Практическая работа №1 Понятия информационной	ОК 01 ОК 02 ОК 09 ПК 3.5		

	безопасности. Угрозы информационной безопасности			
Тема 1.2. Управление безопасностью информации	Лабораторная работа №1 Информационная безопасность. Моделирование угроз	ОК 01 ОК 02 ОК 09 ПК 3.7		
Тема 1.3. Криптография	Практическая работа №2 Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	ОК 01 ОК 02 ОК 09 ПК 3.1		
Тема 1.4. Защита сетевой инфраструктуры	Лабораторная работа №2 Правовые и нормативные основы информационной безопасности	ОК 01 ОК 02 ОК 09 ПК 3.3		
Тема 1.5. Безопасность приложений	Практическая работа №3 Тестирование на проникновение и анализ уязвимостей.	ОК 01 ОК 02 ОК 09 ПК 3.3		
Тема 1.6. Защита данных	Лабораторная работа №3 Криптографические методы защиты. Шифрование данных	ОК 01 ОК 02 ОК 09 ПК 3.2		
Тема 1.7. Безопасность облачных технологий	Практическая работа №4 Изучение модели облачных услуг и их безопасности	ОК 01 ОК 02 ОК 09 ПК 3.1		
Тема 1.8. Инциденты безопасности	Лабораторная работа №4 Управление	ОК 01 ОК 02 ОК 09 ПК 1.5		

	учетными записями и политиками безопасности в Windows			
Тема 1.9. Социальная инженерия и человеческий фактор	Практическая работа №5 Разработка политики информационной безопасности	ОК 01 ОК 02 ОК 09 ПК 1.1		
Тема 1.10. Будущее информационной безопасности	Лабораторная работа №5 Защита от вредоносного программного обеспечения. Антивирусы	ОК 01 ОК 02 ОК 09 ПК 1.4		
Тема 1.11. Киберугрозы будущего: ИИ и машинное обучение в информационной безопасности	Практическая работа №6 Создание реферат на тему киберугрозы будущего	ОК 01 ОК 02 ОК 09 ПК 1.3		
Тама 1.12. Кибероружие и его влияние на глобальную безопасность	Лабораторная работа №6 Сетевая безопасность. Межсетевые экраны	ОК 01 ОК 02 ОК 09 ПК 1.3		

2. Оценочные средства текущего контроля успеваемости и критерии оценки
Вопросы к контрольным срезам

Контрольный срез № 1

Вариант 1

1. Что из перечисленного НЕ является основным свойством информации с точки зрения информационной безопасности?
   а) Конфиденциальность
   б) Доступность
   в) Актуальность
   г) Целостност

2. Как называется необратимое преобразование данных в строку фиксированной

длины, используемое для хранения паролей?
а) Шифрование
б) Кодирование
в) Хэширование
г) Дешифрование

3. Какой нормативно-правовой акт регулирует обработку персональных данных в Российской Федерации?
а) Уголовный кодекс РФ
б) ФЗ-152 «О персональных данных»
в) Доктрина информационной безопасности РФ
г) ФЗ-149 «Об информации, информационных технологиях...»

4. Что из перечисленного является примером атаки с использованием методов социальной инженерии?
а) Фишинговое письмо, якобы от имени банка
б) DDoS-атака на сайт компании
в) Вирус-шифровальщик, попавший через флешку
г) Перехват трафика в публичной сети Wi-Fi

5. Какой тип алгоритмов шифрования использует один и тот же ключ для шифрования и дешифрования данных?
а) Симметричный
б) Асимметричный
в) Хэш-функция
г) Квантовый

6. Для чего используется брандмауэр (межсетевой экран)?
а) Для поиска вирусов на жестком диске
б) Для фильтрации сетевого трафика на основе заданных правил
в) Для создания резервных копий данных
г) Для шифрования файлов и папок

7. Какой из этих стандартов безопасности напрямую относится к индустрии платежных карт?
а) GDPR
б) HIPAA
в) PCI DSS
г) ISO 27001

8. Какая программа классифицируется как вредоносное ПО (ВПО)?
а) Текстовый редактор
б) Графический редактор

в) Троянский конь
г) Электронная таблица

9. Какая мера защиты наиболее эффективна против атак, использующих подбор пароля (брутфорс)?
а) Установка антивируса
б) Регулярное обновление ПО
в) Настройка блокировки учетной записи на несколько неудачных попыток
г) Использование файрвола

10. Что из перечисленного является примером реализации угрозы «Отказ в обслуживании» (DoS)?
а) Кража базы данных клиентов
б) Многократная отправка запросов к серверу, вызывающая его зависание
в) Изменение данных в платежной ведомости
г) Получение доступа к чужой электронной почте

Вариант 2

1. Что подразумевается под термином «целостность информации»?
а) Информация доступна только авторизованным пользователям
б) Информация не была изменена или уничтожена несанкционированным образом
в) Информация всегда доступна авторизованным пользователям по первому требованию
г) Информация представлена в цифровом виде

2. Какой метод защиты наиболее эффективен против вирусов-шифровальщиков (ransomware)?
а) Использование сложного пароля
б) Регулярное создание резервных копий (backup) на изолированном носителе
в) Включение брандмауэра Windows
г) Настройка двухфакторной аутентификации

3. Какая информация НЕ относится к специальной категории персональных данных согласно ФЗ-152?
а) Расовая принадлежность
б) Политические взгляды
в) Состояние здоровья
г) Фамилия, имя, отчество

4. Какой из этих стандартов безопасности регулирует защиту медицинской

информации в США?

а) GDPR

б) HIPAA

в) PCI DSS

г) COPPA

5. Что из перечисленного является примером симметричного алгоритма шифрования?

а) AES

б) RSA

в) SHA-256

г) Diffie-Hellman

6. Как называется тип атаки, при которой злоумышленник подбирает пароль, перебирая все возможные комбинации символов?

а) Фишинг

б) MITM

в) Брутфорс (Brute force)

г) Спуфинг

7. Что произойдет с файлом, если изменить его расширение с .docx на .pdf?

а) Он станет PDF-файлом и откроется в Adobe Reader

б) Он останется документом Word, но система может ошибиться при попытке его открыть

в) Он автоматически сконвертируется в PDF

г) Файл будет удален антивирусом

8. Главная цель использования «песочницы» (sandbox) в системах безопасности?

а) Ускорить работу компьютера

б) Зашифровать все данные пользователя

в) Изолировать и запустить подозрительную программу в безопасной среде без риска для основной системы

г) Создать резервную копию системы

9. Какая функция отвечает за то, чтобы пользователь не мог установить программное обеспечение без прав администратора в Windows?

а) Windows Defender

б) Групповая политика

в) Контроль учетных записей (UAC)

г) Брандмауэр

10. Какой метод криптографии используется для проверки целостности

сообщения и подтверждения, что оно отправлено именно заявленным отправителем?

а) Симметричное шифрование
б) Асимметричное шифрование
в) Электронная подпись
г) Хэширование без ключа

Критерии оценивания компетенций

Оценка(стандартная)	**Баллы**	**%правильных ответов**
«отлично»	20 баллов	76-100 %
«хорошо»	15 баллов	51-75%
«удовлетворительно»	10 баллов	25-50%
«неудовлетворительно»	5 баллов	менее 25%

3. Оценочные средства для промежуточной аттестации и критерии оценки

Вопросы к экзамену

1. Понятие информационной безопасности (ИБ). Основные составляющие ИБ: конфиденциальность, целостность, доступность.
2. Классификация угроз информационной безопасности. Источники угроз.
3. Понятия «уязвимость» и «атака». Взаимосвязь угроз, уязвимостей и атак.
4. Модель угроз: определение, цель построения, основные этапы.
5. Нормативно-правовая база ИБ в РФ: Конституция РФ, Доктрина ИБ, ФЗ-149 «Об информации...».
6. Федеральный закон «О персональных данных» (ФЗ-152): основные понятия, права субъекта, обязанности оператора.
7. Уголовная ответственность за преступления в сфере компьютерной информации (Глава 28 УК РФ).
8. Понятие и цели криптографии. Симметричное и асимметричное шифрование: принципы, плюсы и минусы, примеры.
9. Хэш-функции: назначение, свойства, примеры. Применение для хранения паролей и контроля целостности.
10. Электронная подпись: понятие, принцип работы, правовое регулирование (ФЗ-63).
11. Стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos, HTTPS, OAuth).
12. Сетевая безопасность. Типовые сетевые атаки (DDoS, MITM) и методы защиты от них.

13. Межсетевые экраны (брандмауэры): назначение, принципы работы, типы, примеры правил фильтрации.

14. Вредоносное программное обеспечение (ВПО): классификация (вирусы, черви, трояны, шифровальщики).

15. Принципы работы антивирусных средств (сигнатурный, эвристический анализ, проактивная защита).

16. Управление доступом. Аутентификация, авторизация, администрирование.

17. Методы аутентификации: по паролю, по сертификату, биометрическая, двухфакторная.

18. Безопасность операционных систем. Управление учетными записями и политиками безопасности в Windows.

19. Аудит безопасности. Анализ журналов событий (event logs).

20. Обеспечение безопасности веб-приложений. Основные уязвимости (OWASP Top Ten).

21. Понятие инцидента ИБ. Реагирование на инциденты и цифровая криминалистика (форензика).

22. Защита данных: шифрование данных в покое и в транзите. Резервное копирование.

23. Социальная инженерия: психология атак, основные методы и способы противодействия.

24. Безопасность мобильных приложений: основные угрозы и методы защиты.

25. Международные стандарты и законодательство в области ИБ (GDPR, HIPAA, PCI DSS).

26. Тестирование на проникновение (пентест): цели, этапы, виды.

27. Инструменты обеспечения безопасности: SIEM-системы, DLP-системы, IDS/IPS.

28. Кибербезопасность в облачных средах. Модели ответственности (IaaS, PaaS, SaaS).

29. Тенденции развития ИБ: искусственный интеллект (AI) и машинное обучение (ML) в защите и в атаках.

30. Кибероружие и государственные киберугрозы: понятие, примеры, международное регулирование.

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если глубоко и прочно усвоившему программный, в том числе лекционный материал, последовательно, четко и самостоятельно (без наводящих вопросов) отвечающему на вопрос билета.

Оценка «хорошо» выставляется студенту, твердо знающему программный, в том числе лекционный материал, грамотно и по существу отвечающему на вопрос билета и не допускающему при этом существенных неточностей

(неточностей, которые не могут быть исправлены наводящими вопросами или не имеют важного практического значения). То же относится к освещению практически важных вопросов.

Оценка «удовлетворительно» выставляется студенту, который обнаруживает знание основного материала, но не знает его деталей, допускает неточности, недостаточно правильные формулировки, излагает материал с нарушением последовательности, отвечает на практически важные вопросы с помощью или поправками экзаменатора.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного, в том числе лекционного материала.

Таблица 2 – Ключи к вопросам фонда оценочных средств

№	Компетенция	Содержание вопроса	Правильный ответ
	Контрольный срез № 1 (Вариант1)		
1.	ПК 1.5	Что из перечисленного НЕ является основным свойством информации с точки зрения информационной безопасности? а) Конфиденциальность б) Доступность в) Актуальность г) Целостность	в
2.	ПК 1.5	Как называется необратимое преобразование данных в строку фиксированной длины, используемое для хранения паролей? а) Шифрование б) Кодирование в) Хэширование г) Дешифрование	в
3.	ПК 3.3	Какой нормативно-правовой акт регулирует обработку персональных данных в Российской Федерации? а) Уголовный кодекс РФ б) ФЗ-152 «О персональных данных» в) Доктрина информационной безопасности РФ г) ФЗ-149 «Об информации, информационных технологиях...»	б
4.	ПК 1.5	Что из перечисленного является примером атаки с использованием методов социальной инженерии? а) Фишинговое письмо, якобы от имени банка б) DDoS-атака на сайт компании в) Вирус-шифровальщик, попавший через флешку г) Перехват трафика в публичной сети Wi-Fi	а

5.	ПК 3.3	Какой тип алгоритмов шифрования использует один и тот же ключ для шифрования и дешифрования данных? а) Симметричный б) Асимметричный в) Хэш-функция г) Квантовый	а
6.	ПК 3.3	Для чего используется брандмауэр (межсетевой экран)? а) Для поиска вирусов на жестком диске б) Для фильтрации сетевого трафика на основе заданных правил в) Для создания резервных копий данных г) Для шифрования файлов и папок	б
7.	ПК 1.5	Какой из этих стандартов безопасности напрямую относится к индустрии платежных карт? а) GDPR б) HIPAA в) PCI DS г) ISO 27001	в
8.	ПК 1.5	Какая программа классифицируется как вредоносное ПО (ВПО)? а) Текстовый редактор б) Графический редактор в) Троянский конь г) Электронная таблица	в
9.	ПК 3.3	Какая мера защиты наиболее эффективна против атак, использующих подбор пароля (брутфорс)? а) Установка антивируса б) Регулярное обновление ПО в) Настройка блокировки учетной записи на несколько неудачных попыток г) Использование файрвола	в
10.	ПК 1.5	Что из перечисленного является	б

		примером реализации угрозы «Отказ в обслуживании» (DoS)? а) Кража базы данных клиентов б) Многократная отправка запросов к серверу, вызывающая его зависание в) Изменение данных в платежной ведомости г) Получение доступа к чужой электронной почте	
	Контрольный срез № 1 (Вариант 2)		
1.	ПК 1.5	Что подразумевается под термином «целостность информации»? а) Информация доступна только авторизованным пользователям б) Информация не была изменена или уничтожена несанкционированным образом в) Информация всегда доступна авторизованным пользователям по первому требованию г) Информация представлена в цифровом виде	б
2.	ПК 3.3	Какой метод защиты наиболее эффективен против вирусов-шифровальщиков (ransomware)? а) Использование сложного пароля б) Регулярное создание резервных копий (backup) на изолированном носителе в) Включение брандмауэра Windows г) Настройка двухфакторной аутентификации	б
3.	ПК 3.3	Какая информация НЕ относится к специальной категории персональных данных согласно ФЗ-152? а) Расовая принадлежность б) Политические взгляды в) Состояние здоровья г) Фамилия, имя, отчество	г
4.	ПК 1.5	Какой из этих стандартов безопасности регулирует	б

		защиту медицинской информации в США? а) GDPR б) HIPAA в) PCI DSS г) COPPA	
5.	ПК 1.5	Что из перечисленного является примером симметричного алгоритма шифрования? а) AES б) RSA в) SHA-256 г) Diffie-Hellman	а
6.	ПК 1.5	Как называется тип атаки, при которой злоумышленник подбирает пароль, перебирая все возможные комбинации символов? а) Фишинг б) MITM в) Брутфорс (Brute force) г) Спуфинг	в
7.	ПК 1.5	Что произойдет с файлом, если изменить его расширение с .docx на .pdf? а) Он станет PDF-файлом и откроется в Adobe Reader б) Он останется документом Word, но система может ошибиться при попытке его открыть в) Он автоматически сконвертируется в PDF г) Файл будет удален антивирусом	б
8.	ПК 3.3	Главная цель использования «песочницы» (sandbox) в системах безопасности? а) Ускорить работу компьютера б) Зашифровать все данные пользователя в) Изолировать и запустить подозрительную программу в безопасной среде без риска для основной системы г) Создать резервную копию системы	в
9.	ПК 1.5	Какая функция отвечает за то, чтобы пользователь не мог установить программное	в

		обеспечение без прав администратора в Windows? а) Windows Defender б) Групповая политика в) Контроль учетных записей (UAC) г) Брандмауэр	
10.	ПК 1.5	Какой метод криптографии используется для проверки целостности сообщения и подтверждения, что оно отправлено именно заявленным отправителем? а) Симметричное шифрование б) Асимметричное шифрование в) Электронная подпись г) Хэширование без ключа	в