

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

**УТВЕРЖДАЮ**  
Зав. кафедрой СУиИТ

\_\_\_\_\_ И.М.Першин  
« \_\_\_ » \_\_\_\_\_ 201\_ г.

## **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

для проведения текущей и промежуточной аттестации

По дисциплине	<b>ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ</b>
Направление подготовки	<b>08.03.01</b>
Профиль подготовки	Строительство
Квалификация выпускника	Бакалавр
Форма обучения	очная
Учебный план	2020

Объем занятий: Итого 27 ч. 1 з.е.

В том числе аудиторных 12 ч.

Из них:

Лекций 12 ч.

Лабораторных работ - ч.

Практических занятий –ч.

Самостоятельной работы 15 ч.

Зачет 2 семестр

Дата разработки: « \_\_\_ » \_\_\_\_\_ 20\_\_\_ г.

## Предисловие

1. Назначение: для проверки знаний, умений и навыков текущего и промежуточного контроля.
2. Фонд оценочных средств текущего контроля и промежуточной аттестации составлен на основе рабочей программы дисциплины в соответствии с образовательной программой по направлению подготовки **08.03.01 Строительство**, утвержденной на заседании учебно-методического совета ФГАОУ ВО «СКФУ», протокол №\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г.
3. Разработчик \_\_\_\_\_ Мишин В.В., доцент кафедры СУиИТ
4. ФОС рассмотрен и утвержден на заседании кафедры систем управления и информационных технологий, протокол №\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г.

ФОС согласован с выпускающей кафедрой конституционного и административного права, протокол №\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г.

---

5. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель \_\_\_\_\_ Першин И.М.  
\_\_\_\_\_ Антонов В.Ф.  
\_\_\_\_\_ Сорокин И.Д.

Экспертное заключение: данные оценочные средства соответствуют требованиям федерального государственного образовательного стандарта высшего образования, рекомендуются для использования в учебном процессе.

«\_\_» \_\_\_\_\_ 20\_\_ г. \_\_\_\_\_ И.М.Першин

6. Срок действия ФОС один год.

По дисциплине **ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ**  
 Направление подготовки **08.03.01**  
 Направленность **Строительство**  
 (профиль)  
 Квалификация выпускника **бакалавр**  
 Форма обучения **очная**  
 Год начала обучения **2020**

<b>Код оцениваемой компетенции</b>	<b>Этап формирования компетенции (№ темы)</b>	<b>Средства и технологии оценки</b>	<b>Тип контроля (текущий/промежуточный)</b>	<b>Вид контроля (текущий/промежуточный)</b>	<b>Наименование оценочного средства</b>
ОПК-2	Темы 1, 5	собеседование	текущий	устный	вопросы для собеседования
ОПК-2	Темы 1,2,5,6,7	отчет письменный	текущий	письменный, с помощью технических средств	темы индивидуальных заданий для письменного отчета

Составитель \_\_\_\_\_ Мишин В.В.  
 (подпись)

«\_\_» \_\_\_\_\_ 20\_\_ г.

**УТВЕРЖДАЮ**  
Зав. кафедрой СУиИТ

\_\_\_\_\_ И.М.Першин  
« \_\_\_\_ » \_\_\_\_\_ 201\_ г.

## **Вопросы для собеседования по дисциплине**

### **Персональная кибербезопасность**

#### **Базовый уровень**

#### **Тема 1. Основные понятия персональной кибербезопасности**

1. Информационная безопасность и кибербезопасность.
2. Свойства оцифрованной информации.
3. Причины киберпреступлений.
4. Проблемы кибербезопасности.
5. Анализ рисков как основа управления персональной кибербезопасностью
6. Модель угроз STRIDE.
7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, STRIDE

#### **Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности**

9. Оценка средств криптозащиты.
10. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
11. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
12. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

#### **Повышенный уровень**

#### **Тема 1. Основные понятия персональной кибербезопасности**

13. Основные понятия кибербезопасности.
14. Характеристики оцифрованной информации.
15. Классификация киберпреступлений.
16. Технологии кибербезопасности.
17. Управление персональной кибербезопасностью
18. Характеристики модели угроз STRIDE.
19. Инструменты анализа и контроля информационных рисков.
20. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: Гексада Паркера, 5A, STRIDE

#### **Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности**

21. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций.
22. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.

#### **1. Критерии оценивания компетенций**

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал; все предусмотренные программой задания выполнены, качество их выполнения оценено

числом баллов, близким к максимальному; студент анализирует полученные результаты, проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки. При ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

## **2. Описание шкалы оценивания**

Максимально возможный балл за весь текущий контроль устанавливается равным **55**. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	<b>100</b>
Хороший	<b>80</b>
Удовлетворительный	<b>60</b>
Неудовлетворительный	<b>0</b>

## **3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедура проведения данного оценочного мероприятия включает в себя собеседование по теме. Предлагаемые студенту задания позволяют проверить компетенции ОПК-1, ОПК-3, ПК-8.

Принципиальные отличия заданий базового уровня от повышенного заключаются в том, что задания базового уровня предполагают наличие знаний и умений в области данных компетенций, в то время, как задания повышенного уровня предназначены для демонстрации полного и всеобъемлющего владения знаниями и навыками в области данных компетенций.

Для подготовки к данному оценочному мероприятию необходимо 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными таблицами. При проверке задания оцениваются: последовательность и рациональность выполнения; точность формулировок; знания технологий, использованные при подготовке ответа.

Составитель \_\_\_\_\_ Мишин В.В.  
(подпись)

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

**УТВЕРЖДАЮ**  
Зав. кафедрой СУиИТ

\_\_\_\_\_ И.М.Першин  
« \_\_\_\_ » \_\_\_\_\_ 201\_ г.

**Темы индивидуальных заданий для письменного отчета по дисциплине**  
**Персональная кибербезопасность**

**Базовый уровень**

**Тема 1. Основные понятия персональной кибербезопасности**

1. Информационная безопасность и кибербезопасность.
2. Свойства оцифрованной информации.
3. Причины киберпреступлений.
4. Проблемы кибербезопасности.

**Тема 2. Моделирование угроз персональной кибербезопасности**

5. Анализ рисков как основа управления персональной кибербезопасностью
6. Модель угроз STRIDE.
7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, STRIDE

**Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности**

9. Оценка средств криптозащиты.
10. Экономическое обоснование расходов на обеспечение персональной кибербезопасности.
11. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности.
12. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности.

**Тема 6. Инструменты организации персональной кибербезопасности**

13. Обзор антивирусных средств защиты при организации системы персональной кибербезопасности.
14. Антивирусная защита персональных компьютеров и мобильных устройств.
15. Брандмауэры.
16. Компоненты аппаратных средств защиты информации.

**Тема 7. Персональная кибербезопасность в интернет-банкинге**

17. Интернет-банкинг.
18. Технологии защиты в интернет-банкинге.
19. Причины киберпреступлений в интернет-банкинге.
20. Проблемы кибербезопасности в интернет-банкинге.

**Повышенный уровень**

**Тема 1. Основные понятия персональной кибербезопасности**

1. Основные понятия кибербезопасности.
2. Характеристики оцифрованной информации.
3. Классификация киберпреступлений.
4. Технологии кибербезопасности.

**Тема 2. Моделирование угроз персональной кибербезопасности**

5. Управление персональной кибербезопасностью
6. Характеристики модели угроз STRIDE.

7. Инструменты анализа и контроля информационных рисков.
8. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: Гексада Паркера, 5A, STRIDE

#### **Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности**

9. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций.
10. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.

#### **Тема 6. Инструменты организации персональной кибербезопасности**

11. Средства аппаратной защиты информации.
12. Организация программно-аппаратных средств персональной кибербезопасности.
13. Интернет-банкинг.
14. Технологии защиты в интернет-банкинге.
15. Причины киберпреступлений в интернет-банкинге.
16. Проблемы кибербезопасности в интернет-банкинге.

##### **1. Критерии оценивания компетенций**

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал; все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; студент анализирует полученные результаты, проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки. При ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

##### **2. Описание шкалы оценивания**

Максимально возможный балл за весь текущий контроль устанавливается равным **55**. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	<b>100</b>

Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

**3.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедура проведения данного оценочного мероприятия включает в себя защиту отчета по лабораторной работе.

Предлагаемые студенту задания позволяют проверить компетенции ОПК-1, ОПК-3, ПК-8. Принципиальные отличия заданий базового уровня от повышенного заключаются в том, что задания базового уровня предполагают наличие знаний и умений в области данных компетенций, в то время, как задания повышенного уровня предназначены для демонстрации полного и всеобъемлющего владения знаниями и навыками в области данных компетенций.

Составитель \_\_\_\_\_ Мишин В.В.

«\_\_\_» \_\_\_\_\_ 20\_\_ г.



