МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Технологии обеспечения информационной безопасности
название дисциплины (модуля)

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	Очная
Реализуется в семестре	2

Введение

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Технологии обеспечения информационной безопасности»

2. ФОС является приложением к программе дисциплины «Технологии обеспечения информационной безопасности» в соответствии с образовательной программой по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») по дисциплине «Технологии обеспечения информационной безопасности»

3. Разработчик Петренко В.И, заведующий кафедры

4. Проведена экспертиза ФОС.

Члены экспертизы ФОС;

Председатель: Петренко В.И. – заведующий кафедрой

Члены комиссии: Мандрица И.В., профессор кафедры
Рачков В.Е., доцент кафедры
Жук А.П., профессор кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность (профиль «Информационная безопасность киберфизических систем») и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Технологии обеспечения информационной безопасности».

5. Срок действия ФОС: на срок реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;				
ИД-2 ОПК-1 формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	Не формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	Плохо формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	Хорошо формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	Сразу формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности
ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность	Не умеет разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Почти разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Умеет разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует	Самостоятельно разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает

решений и анализирует показатели деятельности			показатели деятельности	эффективность решений и анализирует показатели деятельности
Компетенция: ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;				
ИД-1 ОПК-2 использует методы концептуального проектирования технологий обеспечения информационной безопасности	Не умеет использует методы концептуального проектирования технологий обеспечения информационной безопасности	Не использует методы концептуального проектирования технологий обеспечения информационной безопасности	Хорошо использует методы концептуального проектирования технологий обеспечения информационной безопасности	Уверенно использует методы концептуального проектирования технологий обеспечения информационной безопасности
ИД-3 ОПК-2 решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Не умеет решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Не достаточно решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Очень хорошо решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Самостоятельно решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 2	
1.	A	Сведения (сообщения, данные) независимо от формы их представления: A. Информация B. Информационные технологии C. Информационная система D. Информационно-телекоммуникационная сеть E. Обладатель информации	ОПК-1
2.	B	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов: A. Информация B. Информационные технологии C. Информационная система D. Информационно-телекоммуникационная сеть E. Обладатель информации	ОПК-1
3.	D	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это: A. База данных B. Информационная технология C. Информационная система D. Информационно-телекоммуникационная сеть	ОПК-1
4.	E	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или	ОПК-1

		договора право разрешать или ограничивать доступ к информации: A. Источник информации B. Потребитель информации C. Уничтожитель информации D. Носитель информации E. Обладатель информации	
5.	A	Информация, переданная или полученная пользователем информационно-телекоммуникационной сети: A. Электронное сообщение B. Информационное сообщение C. Текстовое сообщение D. Визуальное сообщение E. SMS-сообщение	ОПК-1
6.	A	Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это: A. Информационная система персональных данных B. База данных C. Централизованное хранилище данных D. Сервер	ОПК-1
7.	D	Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д это: A. «Исправление персональных данных» B. «Работа с персональными данными» C. «Преобразование персональных данных» D. «Обработка персональных данных»	ОПК-1

		E. «Изменение персональных данных»	
8.	A	Согласно рекомендациям X.800 аутентификация может быть реализована на: A. сетевом уровне B. транспортном уровне C. прикладном уровне	ОПК-1
9.	A, B	В число целей политики безопасности верхнего уровня входят: A. решение сформировать или пересмотреть комплексную программу безопасности B. обеспечение базы для соблюдения законов и правил C. обеспечение конфиденциальности почтовых сообщений	ОПК-1
10.	C	Для безопасной передачи данных по каналам интернет используется технология: A. WWW B. DICOM C. VPN D. FTP E. XML	ОПК-1
11.	C	Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа: A. Антивирус B. -Замок C. Брандма́уэр D. Криптография E. Экспертная система	ОПК-1
12.	A	Несанкционированный доступ к информации это: A. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально B. Работа на чужом компьютере без разрешения его владельца	ОПК-1

		C. Вход на компьютер с использованием данных другого пользователя D. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей E. Доступ к СУБД под запрещенным именем пользователя	
13.	A	«персональные данные» это: A. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу B. Фамилия, имя, отчество физического лица C. Год, месяц, дата и место рождения, адрес физического лица D. Адрес проживания физического лица E. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»	ОПК-1
14.	E	В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности: A. Выход в Интернет без разрешения администратора B. При установке компьютерных игр C. В случаях установки нелицензионного ПО D. В случае не выхода из информационной системы E. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности	ОПК-1
15.	C	Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия: A. Нет, только к административной ответственности B. Нет, если это государственное предприятие C. Да D. Да, но только в случае, если действия сотрудника нанесли непоправимый вред	ОПК-1

		E. Да, но только в случае осознанных неправомочных действий сотрудника	
16.	A	Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru: A. Нет, не при каких обстоятельствах B. Нет, но для отправки срочных и особо важных писем можно C. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера D. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем E. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно	ОПК-1
17.	C	Для того чтобы снизить вероятность утраты информации необходимо: A. Регулярно производить антивирусную проверку компьютера B. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок C. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты) D. Защитить вход на компьютер к данным паролем E. Проводить периодическое обслуживание ПК	ОПК-1
18.	A	Пароль пользователя должен A. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания B. Содержать только цифры C. Содержать только буквы D. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.) E. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.	ОПК-1
19.	E	Доступ к информации – это:	ОПК-2

		A. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя B. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц C. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц D. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети E. Возможность получения информации и ее использования	
20.	A	Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это: A. Конфиденциальная информация B. Документы офера и договоров C. Факс D. Личный дневник E. Законы РФ	ОПК-2
21.	A, B	Самыми опасными источниками внутренних угроз являются: A. некомпетентные руководители B. обиженные сотрудники C. любопытные администраторы	ОПК-2
22.	C	Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности. A. просчеты при администрировании информационных систем B. необходимость постоянной модификации информационных систем C. сложность современных информационных систем	ОПК-2
23.	B	Для внедрения логических бомб чаще всего используются ошибки типа: A. отсутствие проверок кодов возврата **B.** переполнение буфера C. нарушение целостности транзакций	ОПК-2
24.	B	Окно опасности появляется, когда: A. становится известно о средствах использования уязвимости	ОПК-2

		B. появляется возможность использовать уязвимость C. реализована угроза	
25.	A, C	Уголовный кодекс РФ предусматривает наказания за: A. создание, использование и распространение вредоносных программ B. ведение личной корреспонденции на производственной технической базе C. нарушение правил эксплуатации информационных систем	ОПК-2
26.	B	Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают: A. средства выявления злоумышленной активности B. средства обеспечения отказоустойчивости C. средства контроля эффективности защиты информации	ОПК-2
27.	A, B	Уровень безопасности B согласно «Оранжевой книге» характеризуется: A. произвольным управлением доступом B. принудительным управлением доступом C. верифицируемой безопасностью	ОПК-2
28.	A, C	В число классов требований доверия безопасности «Общих критериев» входят: A. разработка B. оценка профиля защиты C. сертификация	ОПК-2
29.	B	Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы: A. периметр безопасности B. метки безопасности C. сертификаты безопасности	ОПК-2
30.	B	Согласно рекомендациям X.800 выделяются следующие сервисы безопасности: A. управление квотами B. управление доступом C. экранирование	ОПК-2
31.	C	Уровень безопасности A согласно «Оранжевой книге» характеризуется: A. произвольным управлением доступом B. принудительным управлением доступом C. верифицируемой безопасностью D. устанавливается новое ПО	ОПК-2
32.		Информация - фактор существования и развития общества.	ОПК-2

33.		Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права.	ОПК-2
34.		Термины и определения в области защиты информации.	ОПК-2
35.		Международная нормативная база обеспечения безопасности.	ОПК-2
36.		Правовые основы использования персональных данных.	ОПК-2
37.		Понятие информационной безопасности. Основные составляющие.	ОПК-2
38.		Средства антивирусной защиты	ОПК-2
39.		Идентификация и аутентификация пользователей. Парольная аутентификация. Система S/KEY.	ОПК-2
40.		VPN сетевого уровня. Протокол IPSec.	ОПК-2

2.Описание шкалы оценивания

Оценка «отлично» выставляется обучающемуся, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретного задания, свободнобез затруднений справился с поставленным заданием, показав владение разносторонними приемами и навыками его выполнения, не допустил ошибок и неточностей.

Оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал умение применять полученные знания на практике через решение конкретного задания, справился с поставленным заданием, показав владение необходимыми приемами и навыками его выполнения, при этом допустил не более одной ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретного задания, с трудом справился с поставленным заданием, при этом допустил не более двух ошибок

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретного задания, не справился с поставленным заданием или допустил при его решении трии более серьезные ошибки.

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности; самостоятельно разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности; уверенно использует методы концептуального проектирования технологий обеспечения информационной безопасности; самостоятельно решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Оценка «хорошо» выставляется, если студент продемонстрировал умение формировать актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности; разрабатывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности; использует методы концептуального проектирования технологий обеспечения информационной безопасности; решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение формировать актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности; в основном разрабатывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, не достаточно оценивает

эффективность решений и анализирует показатели деятельности; использует не все методы концептуального проектирования технологий обеспечения информационной безопасности; не достаточно хорошо решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Оценка «неудовлетворительно» выставляется, если студент не формирует актуальную модель угроз для автоматизированных информационных систем и не учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности; не разрабатывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, не достаточно оценивает эффективность решений и анализирует показатели деятельности; не использует все методы концептуального проектирования технологий обеспечения информационной безопасности; не решает типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью