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
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Противодействие распространению и воздействию вредоносного программного обеспечения и поведенческий анализ

Направления подготовки	02.04.01 Математика и компьютерные науки
Направленность (профиль)	Искусственный интеллект в кибербезопасности
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	3

Предисловие

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Противодействие распространению и воздействию вредоносного программного обеспечения и поведенческий анализ».

2. ФОС является приложением к программе дисциплины «Противодействие распространению и воздействию вредоносного программного обеспечения и поведенческий анализ».

3. Разработчики:

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Бабенко М. Г.– зав. кафедрой вычислительной математики и кибернетики

Члены комиссии:
Лапина М. А. – доцент кафедры вычислительной математики и кибернетики
Пелешенко Т. А. – доцент кафедры вычислительной математики и кибернетики

Экспертное заключение: фонд оценочных средств рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Противодействие распространению и воздействию вредоносного программного обеспечения и поведенческий анализ».
«___»_____2026 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенци(ий)			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	**Минимальный уровень (удовлетворительно) 3 балла**	**Средний уровень (хорошо) 4 балла**	**Высокий уровень (отлично) 5 баллов**
Компетенция: **ПК-8 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники**				
Результаты обучения по дисциплине (модлю): ИД-1$_{ПК-8}$ С помощью современных информационных технологий, исследует вновь создаваемые математические модели в естественных науках промышленности;	Используются неэффективные или устаревшие информационные технологии, что приводит к созданию неточных или неполных математических моделей. Модели не соответствуют современным стандартам и не учитывают ключевые параметры, необходимые для решения задач. Отсутствуют или неадекватно применяются подходящие программные средства и инструменты для анализа. Анализ моделей поверхностный или не выполняется, результаты исследования не имеют значимости или полезности.	Используются базовые или устаревшие методы информационных технологий для исследования математических моделей. Модели созданы с учетом основных принципов, но имеют недостаточную точность или не учитывают все возможные переменные. Использование программных средств ограничено стандартными функциями, без глубокого анализа данных. Применяются простые подходы к решению задач, результаты исследования остаются поверхностными, не давая новых предложений или	Используются современные информационные технологии для исследования математических моделей, однако некоторые аспекты могут быть не до конца проработаны. Модели соответствуют основным принципам и стандартам, но могут быть улучшены с точки зрения точности и применения дополнительных методов анализа. Применяются актуальные программы и алгоритмы, но могут быть использованы более подходящие инструменты для конкретных задач. Результаты анализа показывают хорошие выводы, но не всегда поддерживаются дополнительными гипотезами или предложениями по	Использует передовые информационные технологии для исследования и создания математических моделей в различных областях естественных наук и промышленности. Модели разработаны с высокой точностью и соответствуют актуальным научным и техническим требованиям. Процесс исследования включает комплексный анализ данных, оптимизацию моделей и использование специализированных программных средств. На основе полученных результатов предлагаются новые гипотезы или улучшения существующих моделей, что демонстрирует глубокое понимание предмета. Обеспечивается высокий уровень

				детализации и точности представления
Результаты обучения по дисциплине (модулю): ИД-2$_{ПК-8}$ Проводит Параллельные компьютерные и сетевые технологии в рамках профессиональной деятельности	Не использует параллельные компьютерные и сетевые технологии или применяет их с минимальной эффективностью. Знания и навыки недостаточны для решения профессиональных задач с использованием этих технологий. Технологии не применяются должным образом, что ведет к значительным ошибкам или неэффективности работы. Нет учета важных аспектов, таких как производительность, надежность или безопасность при использовании параллельных вычислений и сетевых решений.	Использует параллельные компьютерные и сетевые технологии, но сталкивается с трудностями при их применении. Знания и навыки позволяют решать только базовые задачи или применять стандартные решения без учета специфики и особенностей рабочих процессов. Использование технологий ограничено, может возникать необходимость в дополнительных усилиях для достижения нужных результатов. В процессе работы могут быть замечены ошибки, связанные с недостаточной проработкой параллельных вычислений или сетевых взаимодействий.	Успешно использует параллельные компьютерные и сетевые технологии в своей профессиональной деятельности, применяя их для решения стандартных задач. Технологии используются эффективно, но есть небольшие недочеты в выборе инструментов или алгоритмов. Результаты работы соответствуют основным требованиям, но могут быть оптимизированы. В целом, понимание этих технологий достаточное для решения большинства задач, однако в более сложных ситуациях могут потребоваться дополнительные усилия.	Профессионально использует параллельные компьютерные и сетевые технологии для решения задач в своей деятельности. Демонстрирует глубокие знания и опыт в применении этих технологий для повышения эффективности работы. Применяет передовые методики и решения, оптимизирует процессы и операции, достигая высоких результатов. Использует сложные инструменты и алгоритмы для реализации параллельных вычислений и работы с сетевыми технологиями, обеспечивая высокий уровень надежности и производительности. Знания и навыки позволяют не только выполнять задачи, но и разрабатывать новые подходы и улучшения
Результаты обучения по дисциплине (модулю): ИД-3$_{ПК-8}$ Использует современные языки программирования и пакеты прикладных программ для реализации конкретных алгоритмов и математических моделей	Неэффективно использует современные языки программирования и пакеты прикладных программ, что приводит к значительным ошибкам в реализации алгоритмов и математических моделей. Процесс	Использует базовые или устаревшие языки программирования и пакеты прикладных программ для реализации алгоритмов и математических моделей, что ограничивает возможности и эффективность	Использует современные языки программирования и пакеты прикладных программ для реализации алгоритмов и математических моделей, но иногда выбор инструментов может быть	Использует современные языки программирования и пакеты прикладных программ для реализации сложных алгоритмов и математических моделей. В работе применяются актуальные инструменты и

	разработки может быть неструктурированным или использованы устаревшие и неподходящие инструменты, что снижает производительность и точность решений. Отсутствует понимание правильного выбора инструментов для реализации задач, что ведет к неэффективным результатам.	решения задач. В работе используются Стандартные решения, не всегда подходящие для более сложных или специфичных задач. Реализация алгоритмов и моделей может быть функциональной, но требует доработки с точки зрения оптимизации, производительности и использования актуальных инструментов.	подвержен улучшению или оптимизации. Реализованные решения эффективно решают поставленные задачи, однако в некоторых случаях могут быть использованы более современные или специализированные инструменты. Работы выполнены с достаточной степенью точности и производительности, но некоторые элементы могут требовать доработки или улучшений	технологии, что позволяет достичь высокой производительности, точности и оптимизации решений. Продемонстрированы глубокие знания и умения в различных языках программирования и ПО, а также в выборе наиболее подходящих инструментов для каждой задачи. Работы характеризуются высокой степенью автоматизации и эффективностью реализации, а также наличием новаторских решений.

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
		Семестр 3	
1.	b	Сигнатурный метод антивирусной проверки заключается в a) анализе поведения файла в разных условиях b) сравнении файла с известными образцами вирусов c) отправке файлов на экспертизу в компанию-производителя антивирусного средстваанализе кода на предмет наличия подозрительных команд	ПК8
2.	e	Косвенное проявление наличия вредоносной программы на компьютере a) неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт b) неожиданно появляющееся всплывающее окно с текстом порнографического содержания c) неожиданное отключение электроэнергии d) неожиданное уведомление антивирусной программы об обнаружении вируса e) неожиданное самопроизвольное завершение работы почтового агента	ПК8
3.	d	Антиспамовая программа, установленная на домашнем компьютере, служит для a) корректной установки и удаления прикладных программ b) обеспечения регулярной доставки антивирусной программе новых антивирусных баз c) защиты компьютера от хакерских атак d) защиты компьютера от нежелательной и/или незапрошенной корреспонденции	ПК8
4.	a, b, c	Положения, которые целесообразно вынести в инструкцию по работе за компьютером, разрабатываемую для компьютерного класса средней школы a) не открывать почтовые сообщения от незнакомых отправителей перед работой (копированием, открытие, запуском) с файлами, размещенными на внешнем носителе (компакт-диск, дискета, флеш- накопитель) нужно проверить их на отсутствие вирусов b) перед работой с любым объектом, загруженным из Интернета, его следует проверить на вирусы c) при работе в Интернет не соглашаться на предложения загрузить и/или установить неизвестную программу	ПК8

		d) не открывать почтовые сообщения, содержащие вложения e) не пользоваться определенными видами браузеров	
5.	b	Цель создания анонимного SMTP-сервера – для a) размещения на запрещенной информации b) рассылки спама c) создания ботнета d) распределенных вычислений сложных математических задач	ПК8
6.	d	Метаморфизм – это a) метод маскировки от антивирусов с помощью шифрования b) метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки c) создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд d) создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд	ПК8
7.	a	Деятельность клавиатурных шпионов a) находясь в оперативной памяти, записывают все, что пользователь вводит с клавиатуры и передают своему хозяину b) находясь в оперативной памяти, следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими c) передают хозяину марку и тип используемой пользователем клавиатуры	ПК8
8.	a, b, d	Обязательные свойства любого современного антивирусного комплекса a) не мешать выполнению основных функций компьютера b) не занимать много системных ресурсов c) не занимать канал Интернет d) надежно защищать от вирусов e) быть кроссплатформенным (работать под управлением любой операционной системы) f) интегрироваться в браузер	ПК8

9.	a	Задача, выполняющая модуль планирования, входящий в антивирусный комплекс a) настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.) b) определения параметров взаимодействия различных компонентов антивирусного комплекса c) определения областей работы различных задач поиска вирусов d) настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса	ПК8
10.	d	Логические бомбы относятся к классу a) файловых вирусов b) макровирусов c) сетевых червей d) троянов e) условно опасных программ	ПК8
11.	c	К какому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к … методам антивирусной защиты. a) Теоретическим b) Практическим c) Организационным d) техническим	ПК8
12.	d	Использование брандмауэров относят к … методам антивирусной защиты. a) Теоретическим b) Практическим c) Организационным d) техническим	ПК8
13.	a	К классу условно опасных относятся программы … a) о которых нельзя однозначно сказать, что они вредоносны b) последствия выполнения которых нельзя предугадать c) которые можно выполнять только при наличии установленного антивирусного программного обеспечения d) характеризующиеся способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне)	ПК8

		e) выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны	
14.	c, d	Типы методов антивирусной защиты a) Теоретические b) Практические c) Организационные d) Технические e) программные	ПК8
15.	b	Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами a) более ясный и интуитивно понятный интерфейс b) отсутствие необходимости отдельно покупать его и устанавливать c) наличие более полного функционала	ПК8
16.	a	Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет a) трудности с регулярным автоматическим получением новых антивирусных баз b) невозможность использовать антиспамовую программу в режиме реального времени c) ложные срабатывания в работе персонального брандмауэра d) невозможность запуска антивирусной проверки в режиме реального времени	ПК8
17.	a	Преимущества сигнатурного метода антивирусной проверки над эвристическим a) более надежный b) существенно менее требователен к ресурсам c) не требует регулярного обновления антивирусных баз d) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы	ПК8
18.	a, b, d, e	Типы троянов: a) клавиатурные шпионы b) похитители паролей c) дефрагментаторы дисков d) утилиты скрытого удаленного управления e) логические бомбы f) шутки g) вирусные мистификации	ПК8

19.	a, e	Стадии жизненного цикла классического трояна a) проникновение на чужой компьютер активация b) поиск объектов для заражения c) подготовка копий d) внедрение копий e) выполнение вредоносных действий	ПК8
20.	d	Трояны классифицируются по … a) методу размножения b) методу распространения c) методу маскировки d) типу вредоносной нагрузки	ПК8
21.	a	Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности a) уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer b) уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer c) возможность установить отличную от www.msn.com стартовую страницу d) возможность одновременно работать в нескольких окнах	ПК8
22.	c, d	Преимущества эвристического метода антивирусной проверки над сигнатурным a) более надежный b) существенно менее требователен к ресурсам c) не требует регулярного обновления антивирусных баз d) позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы	ПК8
23.	a	Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает … a) явные проявления b) косвенные проявления c) материальные проявления d) скрытые проявления	ПК8

24.	a, b, c	Скрытые проявлениям вирусного заражения: наличие на рабочем столе подозрительных ярлыков a) наличие в оперативной памяти подозрительных процессов b) наличие на компьютере подозрительных файлов c) подозрительная сетевая активность d) неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт e) неожиданное уведомление антивирусной программы об обнаружении вируса	ПК8
25.	a	Основная задача, которую решает антивирусная проверка в режиме реального времени a) обеспечение непрерывности антивирусной проверки b) обеспечение невмешательства в процесс деятельности других программ c) обеспечение взаимодействия между пользователем и антивирусной программой d) предоставление возможности глубокой проверки заданных объектов	ПК8
26.	a, b	Подозрительная сетевая активность может быть вызвана … a) сетевым червем b) P2P-червем c) Трояном d) логической бомбой	ПК8

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он: предоставляет детальный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет детальный отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; предоставляет детальный отчёт по результатам проведения анализа безопасности компьютерных систем; предоставляет детальный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; предоставляет детальный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет детальный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.

Оценка «хорошо» выставляется студенту, если он: предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем: предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации И анализ результатов; предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.

Оценка «удовлетворительно» выставляется студенту, если он: предоставляет неполный отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; предоставляет неполный отчёт по результатам разработки требований по защите. формирования политик безопасности компьютерных систем и сетей; предоставляет неполный отчёт по результатам проведения анализа безопасности компьютерных систем; предоставляет неполный отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; предоставляет неполный отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; предоставляет неполный отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.

Оценка «неудовлетворительно» выставляется студенту, если он: не предоставляет отчёт по результатам проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации; не предоставляет отчёт по результатам разработки требований по защите, формирования политик безопасности компьютерных систем и сетей; не предоставляет отчёт по результатам проведения анализа безопасности компьютерных систем; не предоставляет отчёт по результатам проведения сертификации программно-аппаратных средств защиты информации и анализ результатов; не предоставляет отчёт по результатам проведения инструментального мониторинга защищенности компьютерных систем и сетей; не

предоставляет отчёт по результатам проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов.