Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 17.06.2026 15:38:47
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

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 аутентификации в информационных системах
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	4

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Технологии аутентификации в информационных системах» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Технологии аутентификации в информационных системах» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Орел Д.В., доцент кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

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

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Технологии аутентификации в информационных системах».

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 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: ПК-1 Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-2 ПК-1 Способен к управлению функционированием СССЭ, защищённостью от НСД сооружений СССЭ*	- затрудняется с пониманием особенностей применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; - затрудняется использовать встроенные механизмы защиты от НСД в составе СССЭ; - не устанавливает и не настраивает программное обеспечение, необходимое для управления СССЭ и средствами защиты от НСД	- в общем понимает особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; - в целом использует встроенные механизмы защиты от НСД в составе СССЭ; - со значительными недочетами устанавливает и настраивает программное обеспечение, необходимое для управления СССЭ и средствами защиты от НСД	- с незначительными замечаниями понимает особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; - с незначительными замечаниями использует встроенные механизмы защиты от НСД в составе СССЭ; - с незначительными замечаниям	- понимает особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; - использует встроенные механизмы защиты от НСД в составе СССЭ; - устанавливает и настраивает программное обеспечение,

			и устанавливает и настраивает программное обеспечение, необходимое для управления СССЭ и средствами защиты от НСД	необходимое для управления СССЭ и средствами защиты от НСД

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 4,	
1.	d	Что такое администрирование? a) процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов b) присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов c) предоставление определённому лицу или группе лиц прав на выполнение определённых действий d) это совокупность действий, обеспечивающих сохранение и/или развитие свойств информационной системы в заданном направлении	ПК-1
2.	d	Что такое аудит? a) процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов b) присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов c) предоставление определённому лицу или группе лиц прав на выполнение определённых действий d) комплекс мероприятий по настройке специального программного обеспечения, которое отслеживает, кто из пользователей выполнил те или иные действия	ПК-1
3.	A, b, c	Назовите процедуры, выполняемые при регистрации пользователя в системе. a) Аутентификация b) Идентификация c) Авторизация d) Аудит e) Администрирование f) Интерпретация	ПК-1

4.	a	Что такое аутентификация? a) процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов b) присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов c) предоставление определённому лицу или группе лиц прав на выполнение определённых действий d) комплекс мероприятий по настройке специального программного обеспечения, которое отслеживает, кто из пользователей выполнил те или иные действия	ПК-1
5.	b	Что такое идентификация? a) процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов b) присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов c) предоставление определённому лицу или группе лиц прав на выполнение определённых действий d) комплекс мероприятий по настройке специального программного обеспечения, которое отслеживает, кто из пользователей выполнил те или иные действия	ПК-1
6.	c	Что такое авторизация? a) процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов b) присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов c) предоставление определённому лицу или группе лиц прав на выполнение определённых действий	ПК-1

		d) комплекс мероприятий по настройке специального программного обеспечения, которое отслеживает, кто из пользователей выполнил те или иные действия	
7.	A, b, c, d	Перечислите элементы аутентификации. a) субъект, который будет проходить процедуру b) характеристика субъекта - отличительная черта c) хозяин системы аутентификации, несущий ответственность и контролирующий её работу d) сам механизм аутентификации, то есть принцип работы системы e) механизм управления доступом, предоставляющий определённые права доступа субъекту	ПК-1
8.	a	Для чего служит механизм управления доступом? a) для предотвращения несанкционированного доступа к информации b) для разграничения прав доступа c) для обеспечения очередности доступа пользователей d) для предотвращения кражи ценностей	ПК-1
9.	A, b, c	Перечислите факторы аутентификации. a) что знает b) чем владеет c) что из себя представляет d) что может сообщить	ПК-1
10.	A, b, c	Приведите примеры факторов аутентификации. a) отпечаток пальца b) пароль c) USB токен d) гарантийное письмо e) история поиска	ПК-1
11.	b, c,	Назовите методы парольной аутентификации. a) одноразовый пароль b) многоразовый пароль c) пин-код d) гарантийное письмо	ПК-1

		e) шифр Цезаря	
12.	c	Приведите пример аутентификации пользователя на основе открытого пароля. a) Пользователь вводит свои имя пользователя «Пользователь» и пароль «qwerty» на рабочей станции. b) Имя пользователя и пароль передаются по сети в открытом виде. c) Сервер аутентификации находит учетную запись пользователя в базе данных аутентификации и сравнивает введенные данные с ее содержимым.	ПК-1
13.	a	Что такое однонаправленные хэш-функции? a) функции, не имеющие обратных функций b) функции, которые при разных аргументах дают один и тот же результат c) функции, которые при одном аргументе могут давать разные результаты	ПК-1
14.	b	Что такое PIN-код? a) буквенно-цифровая последовательность b) цифровая последовательность c) набор любых символов d) уникальный ключ, записанный на USB токен	ПК-1
15.	A, b, c, d	Назовите области и условия использования PIN-кода. a) присутствует только цифровая клавиатура b) нет доступа большого количества людей c) ограниченное число попыток ввода d) наличие дополнительных факторов аутентификации	ПК-1
16.	a	Для чего необходимы парольные политики? a) набор правил, направленных на повышение безопасности компьютера путём поощрения пользователей к использованию надёжных паролей и их правильному использованию b) предотвращение подбора паролей злоумышленником c) предотвращение использования простых паролей d) стимулирование запоминания паролей пользователями e) агитация для переизбрания паролей	ПК-1
17.	A, b, c, d	Приведите примеры атак на системы, в которых используется аутентификация на основе пароля. a) полный перебор паролей	ПК-1

		b) перебор в ограниченном диапазоне c) подбор по словарю d) фишинг e) нейминг f) разбор на символы	
18.	A, b, c, d	Перечислите физиологические биометрические характеристики. a) отпечаток пальца b) рисунок вен ладони c) характеристики голоса d) фото лица e) цвет глаз f) психотип	ПК-1
19.	A, b	Назовите поведенческие биометрические характеристики. a) походка b) клавиатурный почерк c) манера жестикуляции d) скорость речи	ПК-1
20.	A, b	Назовите параметры, определяющие точность биометрических систем. a) ошибки ложного допуска b) ошибки ложного отказа c) ошибки третьего рода d) ошибки позитивного отказа	ПК-1
21.	A, b, d	Приведите примеры атак на системы, использующие аутентификацию с помощью биометрических характеристик. a) фотография лица b) силиконовый муляж отпечатка пальца c) имплант из композитного материала d) контактные линзы с изображением радужной оболочки	ПК-1
22.	a	Что такое одноразовые пароли? a) пароли, предназначенные для использования единожды b) пароли, которые становятся известны злоумышленнику после однократного использования	ПК-1

		c) пароли, состоящие из одного символа	
23.	a	Опишите принцип работы OTP-токенов. a) В основу OTP заложен принцип, что генерируемый пароль действителен для одной сессии. Дополнительно он может быть ограничен по времени b) В основу OTP заложен принцип, что генерируемый пароль действителен до следующей процедуры генерации токена	ПК-1
24.	A, b	Из каких элементов состоит ключевая пара и для чего предназначен каждый элемент? a) открытый и закрытый ключ. С помощью открытого ключа сообщение шифруется, с помощью закрытого – расшифровывается b) открытый и закрытый ключ. С помощью закрытого ключа сообщение подписывается, с помощью открытого – проверяется подпись	ПК-1
25.	A, c	Что такое электронная цифровая подпись? Приведите примеры использования. a) позволяет подтвердить авторство электронного документа b) связана как с автором, так и с самим документом с помощью криптографических методов и не может быть подделана с помощью обычного копирования c) реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость)	ПК-1
26.	A, b	В каких случаях можно использовать криптографию с открытым ключом? a) для шифрования сообщений, передаваемых по открытым каналам связи b) для цифровой подписи электронных документов c) для передачи только незначительных документов d) для систем с открытым исходным кодом	ПК-1
27.	a	Приведите пример использования криптографии с открытым ключом для шифрования сообщения.	ПК-1

		a) С помощью открытого ключа сообщение шифруется, с помощью закрытого – расшифровывается b) С помощью закрытого ключа сообщение шифруется и расшифровыается, открытый ключ используется для проверки целостности c) С помощью закрытого ключа сообщение шифруется, с помощью закрытого открытого – расшифровывается	
28.	a	Приведите пример аутентификации пользователя с помощью открытых ключей. a) С помощью закрытого ключа сообщение подписывается, с помощью открытого – проверяется подпись b) С помощью закрытого ключа сообщение подписывается и проверяется подпись. Открытый ключ используется для контроля целостности c) С помощью открытого ключа сообщение подписывается, с помощью закрытого – проверяется подпись	ПК-1
29.	b	Для чего предназначена инфраструктура открытых ключей (PKI)? a) позволяющих развертывать и управлять одной из наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом b) является хранителем ключей для браузера, обеспечивает защиту различных инфраструктур, включая внутреннюю коммуникацию внутри организаций, Интернета вещей (IoT), одноранговых соединений (P2P) и так далее	ПК-1
30.	A, b, c, d	Назовите способы хранения закрытого ключа. a) смарт-карты b) USB-брелоки c) «таблетки» Touch-Memory d) реестр (в защищённой памяти компьютера)	ПК-1
31.	A, b, c, d	Назовите недостатки аутентификации с помощью открытых ключей. a) Алгоритмы работают очень медленно: примерно в 10 000 раз медленнее симметричных b) Большая требуемая длина ключа c) Проблемы с несколькими получателями, когда сообщение должно быть дополнительно зашифровано d) Средства защиты гибридных процедур	ПК-1

		e) Риск безопасности, доступный для каждого открытого ключа, также является недостатком систем шифрования с открытым ключом	
32.	A, b, c, d, e	Приведите примеры атак на системы, использующие аутентификацию с помощью открытых ключей. a) брутфорс b) частотный анализ c) интерполяция d) понижение e) кросс-протоколы	ПК-1
33.	a	Назовите основные особенности протоколов LAN Manager и NT LAN Manager. a) работает в локальных сетях b) работает в сети Интернет c) включает механизмы подтверждения подлинности пользователя и защиты от атаки «человек посередине»	ПК-1
34.	A, b, c, d	Приведите примеры атак на системы, использующие аутентификацию с помощью протоколов LANMAN и NTLM. a) Прослушивание сетевого трафика b) Подмена сервера c) Подмена пакетов аутентификации d) Подмена метки времени	ПК-1
35.	A, b	Перечислите преимущества протокола Kerberos. a) Безопасность: Kerberos никогда не передает пароли по сети. Вместо этого Kerberos подтверждает личность пользователя, отправляя ограниченные по времени криптографические сообщения, которые становятся недействительными по истечении установленного периода. Даже сообщения были перехвачены и расшифрованы, они были бы бесполезны в считанные минуты. b) Единый вход: Kerberos требует, чтобы пользователь вводил пароль только один раз при первой аутентификации клиента. С этого момента пользователь имеет доступ ко всем керберизованным службам в области Kerberos без необходимости повторно вводить свой пароль. Единый вход	ПК-1

		упрощает работу с несколькими службами, устраняя необходимость в нескольких требованиях входа в систему.	
36.	a	Опишите функции сервера аутентификации, входящего в состав центра распределения ключей протокола Kerberos. a) первая остановка при аутентификации с помощью Kerberos. Сначала клиент должен аутентифицироваться в AS, используя имя пользователя и пароль для входа. b) После этого AS перенаправляет имя пользователя в KDC, который, в свою очередь, предоставляет TGT. Без выполнения этого первого шага клиент не сможет взаимодействовать с какой-либо другой частью системы Kerberos.	ПК-1
37.	A, b, c, d, e	Приведите примеры атак на Kerberos и способы защиты от них. a) Pass-the-ticket: этот метод создает ложный сеансовый ключ путем подделки ложного TGT. Затем хакер может представить TGT службе как действительные учетные данные. Наличие сеансового ключа позволяет этой подделке обходить все этапы проверки Kerberos, которые предшествуют этапу предоставления сеансового ключа. b) Золотой билет: этот метод подделывает билет со статусом администратора. Хакер имеет неограниченный доступ ко всему домену при использовании этого билета; доступны отдельные устройства, серверы, данные и настройки. Хакеры могут создать «золотой билет» только в том случае, если у них есть доступ к машине администратора, обычно через установленное вредоносное ПО. c) Серебряный билет: Подобно атаке Золотого билета, серебряные билеты — это поддельный билет проверки подлинности службы, который предоставляет доступ к службе. Этот метод дает меньший доступ, чем атака по золотому билету, но его также труднее обнаружить. Все взаимодействия на этом этапе являются взаимодействиями клиент / служба, что позволяет хакеру избежать мер безопасности, установленных в KDC. d) Грубая сила: самый очевидный метод, грубая форсировка, включает использование автоматического подбора паролей для ввода тысяч паролей до тех пор, пока не будет найден правильный. Для брутфорса не требуются	ПК-1

		украденные учетные данные, но его легко обнаружить из-за нечеловеческого поведения при входе. e) Вредоносное ПО с скрытым ключом бэкдора : в этом методе хакеры устанавливают скрытый ключ-ключ доступа к бэкдору в систему, чтобы позволить им войти в систему как любой пользователь в любое время в будущем. Этот метод требует ранее успешной атаки Golden Ticket Attack, поскольку эти скелетные ключи могут быть установлены только с административным доступом. Это одни из самых сложных атак для обнаружения, поскольку взлом и атака могут произойти с разницей в годы.	
38.	A, b, c	Какие протоколы включены в механизм аутентификации Point-to-Point Protocol (PPP)? a) Password Authentication Protocol (PAP) b) Challenge Handshake Protocol (CHAP) c) Extensible Authentication Protocol (EAP) d) Web Access Protocol (WAP)	ПК-1
39.	A, b	Перечислите основные элементы стандарта 802.1x. a) аппликант - пользователь, который нуждается в сетевой аутентификации b) сервер аутентификации - обычно RADIUS-сервер, который производит фактическую аутентификацию c) аутентификатор - сетевое устройство, находящееся между аппликантом и сервером аутентификации и предоставляющее доступ в сеть	ПК-1
40.	A, b	Перечислите способы аутентификации при использовании протокола IPSec. a) Туннельный режим b) Транспортный режим c) Агрессивный режим d) Основной режим	ПК-1
41.		Процедуры, выполняемые при регистрации пользователя в системе.	
42.		Понятия аутентификация, идентификация, авторизация.	
43.		Понятие и принципы аудита.	
44.		Методы парольной аутентификации.	
45.		Аутентификация пользователя на основе открытого пароля.	
46.		Однонаправленные хэш-функции.	

47.		PIN-коды. Области и условия использования PIN-кода.	
48.		Элементы аутентификации.	
49.		Факторы аутентификации и их примеры.	
50.		Физиологические биометрические характеристики.	
51.		Поведенческие биометрические характеристики.	
52.		Принцип работы биометрических систем.	
53.		Понятие одноразовые пароли.	
54.		Принцип работы OTP-токенов.	
55.		Аутентификация пользователя при использовании OTP-токеном метода «запрос-ответ».	
56.		Аутентификация пользователя при использовании OTP-токеном метода «только ответ».	
57.		Ключевая пара и предназначение каждого элемента.	
58.		Электронная подпись. Примеры использования.	
59.		Аутентификации пользователя с помощью открытых ключей.	
60.		Предназначение инфраструктуры открытых ключей (PKI).	
61.		Способы хранения закрытого ключа.	
62.		Основные особенности протоколов LAN Manager и NT LAN Manager.	
63.		Типы аутентификации в NTLM.	
64.		Атаки на системы, использующие аутентификацию с помощью протоколов LANMAN и NTLM, и защиты от них.	
65.		Преимущества протокола Kerberos.	
66.		Функции сервера аутентификации, входящего в состав центра распределения ключейпротокола Kerberos.	
67.		Взаимодействие между пользователем, клиентом и сервером RADIUS.	
68.		Метод получения ключей шифрования, используемых для PPP.	
69.		Возможности, которые обеспечивает протокол SSL для безопасности связи.	
70.		Понятие ассоциация безопасности.	

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».

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 показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок

Оценка «хорошо» выставляется, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка;

Оценка «удовлетворительно» выставляется, если студент показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме, были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа;

Оценка «неудовлетворительно» выставляется, студенту, который не знает значительной части программного материала, допускает грубые ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует письменный ответ на вопрос, либо студент отказался его сдавать. _____

**** в соответствии с результатами освоения дисциплины и видами заданий***