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
«Технологии расследования компьютерных преступлений и инцидентов»

Направление подготовки	02.04.01 Математика и компьютерные науки
Профиль	Искусственный интеллект в кибербезопасности
Год начала обучения	2026
Форма обучения	очная
Реализуется в 1 семестре	

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Технологии расследования компьютерных преступлений и инцидентов». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Технологии расследования компьютерных преступлений и инцидентов»

3. Разработчик: кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель

Бабенко М. Г. заведующий кафедрой вычислительной математики и кибернетики

Члены комиссии:

Пелешенко В.С. доцент кафедры вычислительной математики и кибернетики

Пелешенко Т. А. доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя Корниенко С. А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах

Экспертное заключение: фонд оценочных средств соответствует образовательной программе по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

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-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-1. ПК-1.* контролирует соответствие параметров подсистем защиты СССЭ от НСД установленным требованиям, обеспечивает своевременную корректировку настроек СССЭ, средств и систем их защиты от НСД в целях реагирования на выявленные нарушения.	на низком уровне понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД	в основном понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД	понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД	в полном объёме понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД
ИД-2. ПК-1. разрабатывает предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по защите СССЭ от НСД	на низком уровне реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным	в основном реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям	реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ	в полном объёме реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия

	требованиям		от НСД установленным требованиям	параметров подсистем защиты СССЭ от НСД установленным требованиям

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 очная/заочная/очно-заочная	
.	Компьютерная криминалистика занимается сбором и анализом цифровых доказательств, связанных с преступлениями, совершенными с использованием компьютерных технологий. Она включает изучение данных на устройствах и в сетях для выявления преступной деятельности и восстановления удаленной информации, поддерживая расследования и судебные разбирательства.	Что такое компьютерная криминалистика?	ПК-1

2.	Цифровые доказательства — это информация в электронном виде, используемая в судебных разбирательствах и расследованиях, включая данные с компьютеров, мобильных устройств, электронные письма и документы. Их сбор и обработка должны соответствовать строгим стандартам для обеспечения допустимости в суде.	Что такое цифровые доказательства?	ПК-1
3.	данные с компьютеров, мобильных устройств, сети, электронные письма, документы, фотографии и записи.	Какие типы цифровых доказательств существуют?	ПК-1
4.	Точность**,** обширность**, с**корость**,** доступность	Каковы преимущества использования цифровых доказательств в компьютерной криминалистике?	ПК-1

5.	Судебно-техническая экспертиза — это процесс исследования и анализа материалов и объектов с целью предоставления специализированного заключения в суде. Эксперты оценивают доказательства, такие как цифровая информация, документы или физические объекты, чтобы помочь установить факты дела.	Что такое судебно-техническая экспертиза?	ПК-1
6.	Экспертиза цифровых устройств, экспертиза сетевого трафика, экспертиза программного обеспечения, экспертиза электронной почты и сообщений, экспертиза данных.	Какие типы судебно-технических экспертиз существуют в компьютерной криминалистике?	ПК-1

7.	Цифровые улики — это данные и информация, хранящиеся в электронном виде, которые могут быть использованы в качестве доказательств в судебных разбирательствах. Они включают файлы, электронные письма, сообщения, данные из социальных сетей, а также информацию с цифровых устройств, таких как компьютеры и смартфоны.	Что такое цифровые улики?	ПК-1

8.	Цифровые улики можно изъять путем конфискации устройств, таких как компьютеры и смартфоны, а также создания образов данных для анализа. Кроме того, используются специализированные программы для восстановления удаленных файлов и сетевой мониторинг для сбора информации о сетевой активности. Важно соблюдать юридические нормы для обеспечения допустимости улик в суде.	Каким образом можно изъять цифровые улики?	ПК-1

9.	Сетевая атака — это попытка несанкционированного доступа к компьютерным сетям или их компонентам с целью нарушения их работы, кражи данных или нанесения ущерба. Такие атаки могут принимать различные формы, включая DDoS-атаки (распределённые атаки на отказ в обслуживании), вирусные или червячные инфекции, фишинг, а также атаки на уязвимости программного обеспечения. Основная цель сетевых атак — это получение контроля над системой, разрушение её функционирования или кража конфиденциальной информации	Что такое сетевая атака?	ПК-1

10.	Сканирование портов — это процесс проверки доступных портов на компьютере или сервере для определения, какие из них открыты и готовы к соединениям. Этот метод используется как для оценки безопасности сетей администраторами, так и злоумышленниками для поиска уязвимостей. Основные инструменты для сканирования портов включают Nmap и Netcat.	Что такое сканирование портов?	ПК-1

11.	Блокчейн — это децентрализованная и распределенная цифровая книга, которая записывает транзакции в виде цепочки блоков, связанных между собой. Каждый блок содержит информацию о транзакциях и защищен криптографическими методами, что обеспечивает безопасность и неизменность данных. Эта технология лежит в основе криптовалют, таких как Биткойн, и может использоваться в различных сферах, включая финансы, логистику и управление данными.	Что такое блокчейн?	ПК-1

12.	Криптовалюта — это цифровая или виртуальная валюта, использующая криптографию для обеспечения безопасности и анонимности транзакций. Она работает на технологии блокчейн, что позволяет осуществлять децентрализованные и прозрачные финансовые операции без участия посредников, таких как банки. Примеры популярных криптовалют включают Биткойн, Эфир и Лайткойн.	Что такое криптовалюта?	ПК-1

13.	Цифровая подпись — это криптографический метод, который используется для проверки подлинности и целостности цифровых данных. Она создается с помощью закрытого ключа отправителя и может быть проверена с использованием соответствующего открытого ключа, что гарантирует, что данные не были изменены и действительно исходят от указанного отправителя. Цифровые подписи широко применяются в электронных документах, финансовых транзакциях и в системах управления идентификацией.	Что такое цифровая подпись?	ПК-1

14.	При анализе цифровых улик могут быть восстановлены различные типы данных, включая текстовые документы, изображения, видео и аудиофайлы. Также можно извлечь метаданные, такие как время создания и изменения файлов, а также информацию о пользователях и устройствах, которые использовались для доступа к данным. Это позволяет проводить расследования в области кибербезопасности и уголовного права.	Какие типы данных могут быть восстановлены при анализе цифровых улик?	ПК-1

15.	Сниффер — это программное или аппаратное средство, предназначенное для перехвата и анализа сетевого трафика. Он может использоваться как для законных целей, например, для мониторинга сети и диагностики проблем, так и для злоумышленных действий, таких как кража данных или шпионство. Снифферы помогают исследовать, какие данные передаются по сети, и могут выявлять уязвимости в безопасности.	Что такое сниффер?	ПК-1

16.	DDoS-атака (Distributed Denial of Service) — это кибератака, при которой несколько скомпрометированных компьютеров или устройств (ботнет) одновременно направляют большой объем трафика на целевой сервер или сеть, с целью перегрузить их и сделать недоступными для пользователей. Такие атаки могут привести к значительным сбоям в работе сайтов и онлайн-сервисов, а также к финансовым потерям. Защита от DDoS-атак требует комплексного подхода, включая использование специализированных решений и систем фильтрации трафика.	Что такое DDoS-атака?	ПК-1

17.	Методы использования социальных сетей в качестве доказательств могут включать скриншоты постов, комментариев или сообщений, которые подтверждают определенные факты или события. Также могут быть использованы метаданные, такие как время и дата публикации, а также геолокация, если она доступна. Эти данные могут служить важными доказательствами в судебных разбирательствах или расследованиях.	Какие методы использования социальных сетей могут быть использованы в качестве доказательств?	ПК-1

18.	Криптография — это наука о защите информации с помощью методов шифрования, которые делают данные недоступными для несанкционированного доступа. Она используется для обеспечения конфиденциальности, целостности и аутентичности данных, позволяя защищать сообщения и транзакции в цифровом пространстве. Криптография играет ключевую роль в безопасности интернет-коммуникаций и финансовых операций.	Что такое криптография?	ПК-1

19.	В компьютерной криминалистике используются несколько типов криптографии, включая симметричное шифрование, где один и тот же ключ используется для шифрования и дешифрования данных, и асимметричное шифрование, использующее пару ключей (публичный и приватный). Также применяются хэш-функции для проверки целостности данных, которые создают уникальные отпечатки для файлов. Эти методы помогают в восстановлении и анализе данных, а также в обеспечении их безопасности в процессе расследования.	Какие типы криптографии используются в компьютерной криминалистике?	ПК-1

20.	Вредоносное ПО, или малварь, — это программное обеспечение, разработанное с целью причинения вреда компьютерам, сетям или пользователям. Оно может принимать различные формы, включая вирусы, черви, трояны и шпионские программы, и часто используется для кражи данных, разрушения систем или получения несанкционированного доступа. Вредоносное ПО представляет серьезную угрозу для безопасности и конфиденциальности пользователей в цифровом пространстве. 😊	Что такое вредоносное ПО?	ПК-1

21.	Кибершпионаж — это практика сбора конфиденциальной информации о физических или юридических лицах с использованием компьютерных технологий и интернет-сетей. Обычно он осуществляется с целью получения стратегических данных, таких как коммерческие тайны, государственные секреты или личные сведения, и может быть направлен как против отдельных людей, так и против организаций или государств. Кибершпионаж представляет собой серьезную угрозу для безопасности и конфиденциальности в цифровом мире.	Что такое кибершпионаж?	ПК-1

22.	DDoS-атака (распределённая атака отказа в обслуживании) можно определить по резкому увеличению трафика на сервере, что приводит к его перегрузке и недоступности для пользователей. Также можно заметить замедление работы сайта или его полное отключение, а также аномалии в логах, такие как большое количество запросов с одного или нескольких IP-адресов. Мониторинг сетевого трафика и использование специализированных инструментов для анализа могут помочь в выявлении таких атак.	Как можно определить, была ли проведена DDoS-атака?	ПК-1

23.	Виртуальная машина (ВМ) — это программная эмуляция физического компьютера, которая позволяет запускать операционные системы и приложения в изолированной среде на одном физическом устройстве. Она использует гипервизор для управления ресурсами хоста и создания нескольких виртуальных сред, что позволяет эффективно использовать аппаратные ресурсы и тестировать различные конфигурации без риска для основной системы. Виртуальные машины широко применяются в облачных вычислениях, разработке и тестировании программного обеспечения.	Что такое виртуальная машина?	ПК-1

24.	Для анализа цифровых улик используются различные инструменты, такие как EnCase, FTK (Forensic Toolkit) и Autopsy, которые помогают в извлечении, анализе и представлении данных с устройств. Также применяются программы для восстановления данных, такие как Recuva, и сетевые анализаторы, например, Wireshark, для изучения сетевого трафика. Эти инструменты позволяют специалистам по цифровой криминалистике выявлять и исследовать улики в процессе расследования.	Какие инструменты используются для анализа цифровых улик?	ПК-1

25.	Стеганография — это метод скрытия информации внутри других данных, таких как изображения, аудиофайлы или текст, с целью сделать ее незаметной для посторонних. В отличие от шифрования, которое делает информацию недоступной без ключа, стеганография маскирует сам факт существования сообщения. Этот метод часто используется для защиты конфиденциальности и передачи данных в условиях повышенной безопасности.	Что такое стеганография?	ПК-1

26.	Для защиты компьютерной системы от кибератак необходимо использовать антивирусное программное обеспечение и регулярно обновлять его, а также операционную систему и приложения. Важно применять брандмауэры, создавать сложные пароли и использовать двухфакторную аутентификацию для повышения безопасности. Также рекомендуется проводить регулярные резервные копии данных и обучать пользователей основам кибербезопасности.	Как можно защитить компьютерную систему от кибератак?	ПК-1

27.	Компьютерная криминалистика — это область, занимающаяся сбором, анализом и представлением цифровых доказательств для расследования преступлений, связанных с компьютерами и интернетом. Она включает в себя восстановление удаленных данных, анализ сетевых атак и изучение вредоносного ПО. Основная цель компьютерной криминалистики — обеспечить законность и достоверность собранных данных для их использования в судебных процессах.	Компьютерная криминалистика.	ПК-1

28.	Цифровая подпись — это криптографический метод, который используется для проверки подлинности и целостности цифровых данных. Она создается с помощью закрытого ключа отправителя и может быть проверена с использованием соответствующего открытого ключа, что гарантирует, что данные не были изменены и действительно исходят от указанного отправителя. Цифровые подписи широко применяются в электронных документах, финансовых транзакциях и в системах управления идентификацией.	Что такое "цифровая подпись"?	ПК-1

29.	Тип кибератаки, основанный на использовании вредоносных программ, называется "вредоносное ПО" (malware). Оно включает в себя вирусы, черви, трояны и шпионские программы, которые могут повреждать системы, красть данные или получать несанкционированный доступ к ресурсам. Вредоносное ПО часто распространяется через зараженные ссылки, электронные письма или загрузки, что делает защиту от него особенно важной.	Какой тип кибератаки основан на использовании вредоносных программ?	ПК-1

30.	Тип кибератаки, основанный на перехвате информации, передаваемой по сети, называется "атака типа Man-in-the-Middle" (MitM). В ходе этой атаки злоумышленник вмешивается в коммуникацию между двумя сторонами, чтобы перехватить, изменить или подменить передаваемые данные. Такие атаки могут происходить в открытых сетях Wi-Fi и требуют серьезных мер безопасности для защиты информации.	Какой тип кибератаки основан на перехвате информации, передаваемой по сети?	ПК-1

31.	Тип кибератаки, направленный на блокирование доступа к компьютерной системе, называется "атака типа отказ в обслуживании" (DoS). В ходе этой атаки злоумышленник перегружает систему или сеть запросами, что приводит к их недоступности для пользователей. В более сложных вариантах, таких как DDoS (распределенная атака отказа в обслуживании), используется множество зараженных устройств для усиления атаки.	Какой тип кибератаки направлен на блокирование доступа к компьютерной системе?	ПК-1

32.	В компьютерной криминалистике используются несколько типов криптографии, включая симметричное и асимметричное шифрование. Симметричное шифрование, такое как AES, использует один ключ для шифрования и расшифровки данных, в то время как асимметричное шифрование, например RSA, использует пару ключей: открытый и закрытый. Эти методы помогают защитить данные и обеспечить их целостность во время расследований.	Какие типы криптографии используются в компьютерной криминалистике?	ПК-1

33.	Вредоносное ПО (или malware) — это программное обеспечение, созданное с целью нанести ущерб, получить несанкционированный доступ или нарушить работу компьютеров и сетей. Оно может принимать различные формы, включая вирусы, черви, трояны и шпионские программы. Вредоносное ПО может красть личные данные, блокировать доступ к системам или использовать ресурсы устройства для выполнения злонамеренных действий.	Что такое вредоносное ПО?	ПК-1

34.	Вредоносное ПО можно обнаружить с помощью антивирусных программ, которые сканируют файлы и процессы на наличие известных угроз. Также применяются методы мониторинга поведения, которые выявляют аномалии в работе системы, и анализ сетевого трафика для обнаружения подозрительных активностей. Дополнительно, использование инструментов для анализа цифровых следов может помочь в выявлении скрытых вредоносных компонентов.	Какими методами можно обнаружить вредоносное ПО?	ПК-1

35.	Доказательства в цепочке (или цепочка доказательств) — это процесс сбора, хранения и передачи доказательств, чтобы гарантировать их подлинность и целостность в юридических или криминалистических расследованиях. Он включает в себя документирование каждого этапа, начиная с момента обнаружения улик и заканчивая их представлением в суде, чтобы обеспечить их приемлемость и надежность. Такой подход помогает предотвратить манипуляции с доказательствами и гарантирует, что они могут быть использованы в процессе судебного разбирательства.	Что такое доказательства в цепочке?	ПК-1

36.	Киберпреступность — это незаконная деятельность, осуществляемая с использованием компьютеров и интернет-технологий, включая хакерство, кражу личных данных, распространение вредоносного ПО и мошенничество. Она может затрагивать как индивидуальных пользователей, так и организации, нанося значительный финансовый и репутационный ущерб. Киберпреступники используют различные методы для обхода защитных мер и получения доступа к конфиденциальной информации.	Что такое киберпреступность?	ПК-1

37.	Компьютерное преступление — это преступление, в котором компьютер или сеть используются как средство совершения незаконных действий. Это может включать в себя хакерство, кражу данных, распространение вирусов и мошенничество в интернете. Такие преступления могут наносить ущерб как отдельным пользователям, так и организациям, нарушая их безопасность и конфиденциальность.	Что такое компьютерное преступление?	ПК-1

38.	Существует множество видов компьютерных преступлений, включая хакерство, фишинг, распространение вредоносного ПО, кражу личных данных и финансовое мошенничество. Также к ним относятся атаки на системы и сети (например, DDoS-атаки) и использование компьютеров для организации преступной деятельности, такой как торговля наркотиками или оружием. Эти преступления могут иметь серьезные последствия для жертв и общества в целом.	Какие виды компьютерных преступлений существуют?	ПК-1

39.	Цифровой след — это совокупность данных, которые остаются после взаимодействия пользователя с интернетом и цифровыми устройствами. Он включает в себя информацию о посещенных веб-сайтах, активностях в социальных сетях, электронных письмах и даже геолокации. Цифровой след может быть использован для анализа поведения пользователей, но также может представлять угрозу для конфиденциальности и безопасности.	Что такое цифровой след?	ПК-1

40.	Основные задачи расследования компьютерных преступлений включают сбор и анализ цифровых улик, идентификацию и задержание подозреваемых, а также восстановление и защита украденных данных. Кроме того, важно оценить ущерб и предотвратить дальнейшие преступления, а также сотрудничать с другими правоохранительными органами и международными организациями. Эти действия помогают обеспечить справедливость и защиту пользователей от будущих угроз.	Какие основные задачи расследования компьютерных преступлений?	ПК-1

41.	Журнал безопасности — это документ или система, в которой регистрируются события и действия, связанные с безопасностью информационных систем. Он включает в себя записи о попытках доступа, изменениях в конфигурации, инцидентах и других событиях, которые могут повлиять на безопасность сети или данных. Анализ журнала безопасности помогает выявлять угрозы и улучшать защиту информационных ресурсов.	Что такое журнал безопасности?	ПК-1

42.	В журнале безопасности могут содержаться данные о попытках входа в систему, успешных и неудачных аутентификациях, изменениях прав доступа, событиях безопасности, таких как атаки или нарушения, а также информацию о действиях пользователей и администраторов. Кроме того, могут фиксироваться детали о сетевом трафике, использовании приложений и событиях, связанных с физической безопасностью. Эти данные помогают в анализе инцидентов и оценке общей безопасности системы.	Какие данные могут содержаться в журнале безопасности?	ПК-1

43.	Хеш-сумма — это короткая строка фиксированной длины, получаемая в результате применения хеш-функции к данным любого объема. Она служит для проверки целостности данных: если даже малейшее изменение во входных данных произойдет, хеш-сумма изменится, что позволяет выявить возможные искажения или подмены. Хеш-суммы широко используются в криптографии, цифровых подписях и системах хранения данных.	Что такое хеш-сумма?	ПК-1

44.	Хеш-суммы используются при расследовании компьютерных преступлений для проверки целостности и подлинности данных. Они позволяют следователям убедиться, что файлы не были изменены после их захвата, а также помогают идентифицировать известные вредоносные программы и улики, сравнивая хеш-суммы с базами данных. Это делает процесс расследования более надежным и эффективным.	Зачем используется хеш-сумма при расследовании компьютерных преступлений?	ПК-1

45.	Цифровые следы делятся на два основных типа: явные и неявные. Явные следы — это данные, которые пользователи оставляют сознательно, такие как сообщения, фотографии и публикации в социальных сетях. Неявные следы включают информацию, собранную автоматически, например, журналы доступа, куки и метаданные, которые могут быть использованы для анализа поведения пользователей.	Какие виды цифровых следов бывают?	ПК-1

46.	Активный цифровой след — это информация, которую пользователь сознательно создает и оставляет в интернете, взаимодействуя с различными платформами. Это могут быть публикации в социальных сетях, комментарии, загрузка файлов и участие в онлайн-обсуждениях. Такой след легко отслеживается и может быть использован для анализа личности и предпочтений пользователя.	Что такое активный цифровой след?	ПК-1

47.	Пассивный цифровой след — это информация, которая собирается автоматически, без активного участия пользователя. Это может включать данные о посещаемых веб-сайтах, времени, проведенном на них, а также информацию о устройствах и местоположении. Такие данные часто используются для анализа поведения пользователей и таргетирования рекламы.	Что такое пассивный цифровой след?	ПК-1

48.	Прямой цифровой след — это информация, которую пользователь оставляет намеренно и осознанно, например, при регистрации на сайтах, заполнении анкет или публикации контента в социальных сетях. Этот след включает личные данные, такие как имя, адрес электронной почты и другие идентифицирующие сведения. Прямой цифровой след легко связывается с конкретным пользователем и может быть использован для создания профилей и анализа его поведения.	Что такое прямой цифровой след?	ПК-1

49.	Косвенный цифровой след — это информация, которая собирается о пользователе без его прямого участия и часто без его ведома. Это может включать данные о его действиях в интернете, таких как клики, просмотры страниц и взаимодействия с контентом. Такие данные помогают компаниям анализировать поведение пользователей и улучшать свои услуги, но они менее очевидны для самих пользователей.	Что такое косвенный цифровой след?	ПК-1

50.	Для сбора цифровых следов используются различные инструменты, включая куки, веб-аналитику (например, Google Analytics), трекеры и пиксели отслеживания. Эти инструменты помогают отслеживать действия пользователей на сайтах, их предпочтения и поведение в интернете. Кроме того, социальные сети и мобильные приложения также собирают данные о пользователях для создания персонализированного контента и рекламы.	Какие инструменты используются для сбора цифровых следов?	ПК-1

51.	Методология сбора данных при расследовании компьютерных преступлений включает систематический подход к выявлению, сохранению и анализу цифровых доказательств. Это может включать использование специализированных инструментов для извлечения данных из устройств, сетей и облачных хранилищ, а также соблюдение юридических и этических норм для обеспечения допустимости доказательств в суде. Эффективная методология помогает обеспечить целостность данных и минимизировать риск их повреждения или потери.	Что такое методология сбора данных при расследовании компьютерных преступлений?	ПК-1

52.	Методология сбора данных при расследовании компьютерных преступлений включает несколько ключевых этапов: подготовка, идентификация, сбор, анализ и представление доказательств. На первом этапе расследователи планируют действия, затем определяют источники данных, после чего осуществляют сбор и сохранение цифровых доказательств. Наконец, результаты анализа представляются в виде отчетов или свидетельств в суде.	Какие этапы включает методология сбора данных при расследовании компьютерных преступлений?	ПК-1

53.	Хеш-сумма — это уникальный код фиксированной длины, который создается на основе содержимого файла или данных с помощью хеш-функции. Она используется для проверки целостности данных, так как любое изменение в исходном содержимом приведет к изменению хеш-суммы. Хеш-суммы часто применяются в кибербезопасности и цифровой криминалистике для подтверждения подлинности файлов и выявления изменений.	Что такое хеш-сумма?	ПК-1

54.	Хеш-сумма используется в расследовании компьютерных преступлений для проверки целостности и подлинности цифровых доказательств. Она позволяет следователям убедиться, что данные не были изменены или повреждены после их сбора, что критически важно для поддержания доказательственной силы в суде. Кроме того, хеш-суммы помогают идентифицировать и сопоставлять файлы, что облегчает анализ больших объемов данных.	Зачем используется хеш-сумма в расследовании компьютерных преступлений?	ПК-1

55.	При расследовании компьютерных преступлений используются различные программные инструменты, такие как EnCase и FTK, которые помогают в сборе, анализе и хранении цифровых доказательств. Также популярны утилиты для восстановления данных, такие как Recuva и PhotoRec, а также инструменты для анализа сетевого трафика, например Wireshark. Эти программы обеспечивают эффективный и безопасный процесс расследования, позволяя следователям извлекать и анализировать информацию из различных источников.	Какие программные инструменты используются при сборе и анализе данных в расследовании компьютерных преступлений?	ПК-1

56.	Кросс-доменная атака (или кросс-доменная подделка) — это тип уязвимости, при которой злоумышленник может обманом заставить пользователя выполнить нежелательные действия на другом веб-сайте, на который он авторизован. Это может происходить, например, через поддельные формы или ссылки, которые используют доверие пользователя к сайту. Такие атаки могут привести к утечке конфиденциальной информации или несанкционированным действиям от имени пользователя.	Что такое кросс-доменная атака?	ПК-1

57.	SQL-инъекция — это тип уязвимости веб-приложений, при котором злоумышленник вставляет вредоносные SQL-запросы в поля ввода, чтобы манипулировать базой данных. Это может привести к несанкционированному доступу к данным, их изменению или удалению. SQL-инъекции могут серьезно угрожать безопасности системы и конфиденциальности пользователей.	Что такое SQL-инъекция?	ПК-1

58.	DDoS-атака (распределённая атака отказа в обслуживании) — это попытка сделать онлайн-сервис недоступным, перегружая его трафиком от множества скомпрометированных устройств. Злоумышленники используют ботнеты для отправки огромного объема запросов, что приводит к сбоям в работе сервиса. Такие атаки могут вызвать значительные финансовые потери и ущерб репутации компании.	Что такое DDoS-атака?	ПК-1

59.	Для защиты от DDoS-атак можно использовать несколько мер безопасности, таких как внедрение систем фильтрации трафика, которые помогают идентифицировать и блокировать вредоносные запросы. Также стоит рассмотреть использование CDN (систем доставки контента) и облачных сервисов, которые могут распределять нагрузку и смягчать атаки. Регулярное обновление программного обеспечения и мониторинг сетевой активности также играют важную роль в повышении безопасности.	Какие меры безопасности можно предпринять для защиты от DDoS-атак?	ПК-1

60.	Сетевой протокол — это набор правил и стандартов, определяющих, как устройства в сети обмениваются данными. Он регулирует форматы сообщений, порядок их передачи и обработку ошибок, обеспечивая совместимость и эффективное взаимодействие между различными устройствами. Примеры сетевых протоколов включают TCP/IP, HTTP и FTP.	Что такое сетевой протокол?	ПК-1
61.	Wireshark, tcpdump, Snort и другие	Какие инструменты могут использоваться для анализа сетевых протоколов при расследовании компьютерных преступлений?	ПК-1
62.	c) Самостоятельное проведение расследования.	Какую из перечисленных опций НЕ следует выполнять при обнаружении потенциального компьютерного преступления? a) Оповещение соответствующих органов b) Сохранение логов и других данных для последующего анализа c) Самостоятельное проведение расследования d) Обеспечение физической безопасности системы	ПК-1
63.	d) Мобильные приложения.	Что из перечисленного НЕ является примером потенциальных целей для кибератак? a) Банковские аккаунты b) Данные пользователей c) Локальные сети d) Мобильные приложения	ПК-1

64.	b) Изучение криминалистических доказательств, полученных из цифровых устройств и систем.	Что такое "форензический анализ"? a) Исследование документов и файлов, находящихся на сервере b) Изучение криминалистических доказательств, полученных из цифровых устройств и систем c) Процесс взлома учетной записи пользователя d) Метод поиска источников вредоносных программ на веб-сайтах	ПК-1
65.	a) Метод защиты от атак, которые используют множество устройств для отправки трафика на один веб-сервер.	Что такое "защита от DDoS-атак"? a) Метод защиты от атак, которые используют множество устройств для отправки трафика на один веб-сервер b) Метод защиты от атак, при которых злоумышленники пытаются получить доступ к системе путем перебора паролей c) Метод защиты от атак, при которых злоумышленники пытаются перехватить данные, передаваемые между клиентом и сервером d) Метод защиты от атак, при которых злоумышленники используют вредоносные программы, которые перехватывают данные на компьютере пользователя	ПК-1
66.	b) Расследование, проводимое внутри компании или организации	Что такое "внутреннее расследование"? a) Расследование, проводимое правоохранительными органами b) Расследование, проводимое внутри компании или организации c) Расследование, проводимое в отношении иностранных агентов d) Расследование, проводимое по поводу проблем с безопасностью внешней среды.	ПК-1
67.	d) Метод похищения финансовых данных пользователей, который часто используется в отношении банковских карт.	Что такое "скимминг"? a) Метод защиты от взлома посредством перебора паролей b) Метод защиты от атаки DDoS c) Метод защиты от вредоносных программ, которые перехватывают данные на компьютере пользователя d) Метод похищения финансовых данных пользователей, который часто используется в отношении банковских карт	ПК-1

68.	c) Вредоносная программа, которая позволяет злоумышленникам получить удаленный доступк зараженному устройству.	Что такое "бекдор"? a) Вредоносная программа, предназначенная для перехвата данных, передаваемых между клиентом и сервером b) Вредоносная программа, которая перехватывает управление над компьютером пользователя c) Вредоносная программа, которая позволяет злоумышленникам получить удаленный доступ к зараженному устройству d) Вредоносная программа, которая шифрует данные на компьютере пользователя и требует выкупа для их восстановления	ПК-1
69.	a) Совокупность фактов и данных, которые свидетельствуют о том, что преступление было совершено.	Что такое "цепочка доказательств"? a) Совокупность фактов и данных, которые свидетельствуют о том, что преступление было совершено b) Метод, позволяющий защититься от кибератак путем создания нескольких слоев защиты c) Метод, позволяющий противостоять вредоносным программам, которые используют социальную инженерию для получения доступа к учетной записи пользователя d) Система мер, которые позволяют защитить конфиденциальную информацию от несанкционированного доступа	ПК-1

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины.

3. Критерии оценивания компетенций*

Оценка «зачтено» выставляется студенту, если он, в полном объёме понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД, в полном объёме реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям.

Понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД, реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям.

В основном понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД, в основном реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям.

Оценка «не зачтено» выставляется студенту, если он, на низком уровне понимает организацию и содержание мониторинга функционирования СССЭ, их защищенности от НСД, возможные источники и технические каналы утечки информации, реализует методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД, на низком уровне реализует методические документы уполномоченных федеральных органов исполнительной власти по защите информации, проводит контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям.