Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«____»_____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Форензика

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*9*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2020

Разработчик рабочей программы:

(должность, степень, ученое звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

(наименование кафедры)	(подпись)	(ФИО)

1 Общие положения

Рабочая программа дисциплины «Форензика» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Обеспечение информационной безопасности распределенных информационных систем» по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Задачи дисциплины	Приобретение обучаемыми необходимого объёма знаний и практических навыков в области обеспечения информационной безопасности конфиденциальной информации
Основные разделы / темы дисциплины	1. Организация и проведение работ по обработке и защите конфиденциальной информации 2. Обращение со служебной информацией ограниченного доступа на предприятиях

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Форензика» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
Способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	З1 (ПК-5-2) знать основные методы анализа сетевого трафика;	У1 (ПК-5-2) уметь анализировать сетевую инормацию;	Н1 (ПК-5-2) владеть навыком работы с Wireshark по анализу различных протоколов в сети;
Способность обеспечивать эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25)	З2 (ПК-25-4) знать об основных методах исследования компьютерной информации;	У2 (ПК-25-4) уметь анализировать лог файлы операционных систем;	Н2 (ПК-25-4) владеть навыком работы с программой volatility;

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Форензика» изучается на 5 курсе(ах) в 9 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик Внутренний и внешний аудит информационной безопасности, основы информационной безопасности, стандартизация защищенных автоматизированных систем.
Знания, умения и навыки, сформированные при изучении дисциплины «Форензика», будут востребованы при изучении последующих дисциплин: Администрирование распределенных информационных систем

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 з.е., 108 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	32
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	16
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	40
Промежуточная аттестация обучающихся – Экзамен	36

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 1 Исследование сетевого трафика. Теоретические основы исследования сетевого трафика, Исследование мультимедийного трафика Исследование данных передаваемых через протокол TCP	8		8	20

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 2 Исследование компьютерной информации Теоретические основы исследования компьютерной информации Исследование файловых систем операционных систем Исследование ОЗУ	8		8	20
ИТОГО по дисциплине	**16**		**16**	**40**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	10
Подготовка к занятиям семинарского типа	10
Подготовка и оформление РГР	20
	40

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Багмет А.М. Извлечение данных из электронных устройств как самостоятельное следственное действие / А.М. Багмет, С.Ю. Скобелин // Право и кибербезопасность. 2013. N 2. С. 22 - 27.

2. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности / С.Ю. Скобелин // Российский следователь. 2019. N 3. С. 26 - 28.
3. Шеметов А.К. О понятии виртуальных следов в криминалистике / А.К. Шеметов // Российский следователь. 2014. N 20. С. 52 - 54.
4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2014. – 416 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: **http://www.znanium.com/catalog.php**, ограниченный. – Загл. с экрана.
5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2013. – 592 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: **http://www.znanium.com/catalog.php**, ограниченный. – Загл. с экрана.

8.2 Дополнительная литература

1. Крис Сандерс Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях / С. Крис – М. : Диалектика, 2019. – 450 с.
2. Колиснеченко, Д. Серверное применение Linux / Д. Колиснеченко, М. Матвеев, Р. Прокди – Санкт-Петербург : БХВ-Петербург, 2016. – 510 с.
3. Уильям, Р. Windows 7 для продвинутых. Настройка, работа и администрирование/ Р. Уильям – Санкт-Петербург : Питер, 2015. – 576 с.
4. Трент, Р. Unix и Linux. Руководство системного администртора/ Р. Трент – Москва : Горячая Линия - Телеком, 2014. – 352 с.
5. Хилл, Б. Полный справочник по Cisco./ Б. Хилл – Санкт-Петербург : Питер, 2012. – 780 с.
6. Цифровая экономика: 2022 : краткий статистический сборник / Г. И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2022
URL:https://publications.hse.ru/pubs/share/direct/553808040.pdf

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Форензика» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие

	вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Организация и технология защиты конфиденциальной информации в информационных системах» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты РГР;

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+
3. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. Материалы данного курса (9 семестр) выложены на портал ДО КнАГУ и организация взаимодействия в рамках данной дисциплины проводится с привлечением дистанционных технологий.

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Wireshark (ссылка для свободного скачивания «https://www.wireshark.org/#download»)
2. 2. Volatility (ссылка для свободного скачивания

«https://github.com/volatilityfoundation/volatility»)
3. 3. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
4. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению расчетно-графической работы

Теоретическая часть расчетно-графической работы выполняется по установленным темам с использованием практических материалов. К каждой теме расчетно-графической работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
201/5	Учебная лаборатория защищённых автоматизированных систем	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория № 201 , оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Форензика

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*9*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
Способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	З1 (ПК-5-2) знать основные методы анализа сетевого трафика;	У1 (ПК-5-2) уметь анализировать сетевую инормацию;	Н1 (ПК-5-2) владеть навыком работы с Wireshark по анализу различных протоколов в сети;
Способность обеспечивать эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25)	З2 (ПК-25-4) знать об основных методах исследования компьютерной информации;	У2 (ПК-25-4) уметь анализировать лог файлы операционных систем;	Н2 (ПК-25-4) владеть навыком работы с программой volatility;

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
1. Исследование мультимедийного трафика	ПК-5	Лабораторная работа 1	Умение восстановить аудиопоток, переданный через протокол SIP, восстановить видеопоток, выполнить отчет о проделанной работе.
2. Исследование данных передаваемых через протокол TCP	ПК-5	Лабораторная работа 2	Умение в программе Wireshark восстановить информацию, переданную по протоколу FTP, SMB2, HTTP, SMPT, POP3, DNS

3. Исследование файловых систем операционных систем	ПК-25	Лабораторная работа 3	Умение проводить исследование файловых систем операционных систем
4. Исследование ОЗУ	ПК-23	Лабораторная работа 4	Умение сформировать перечень требований к персоналу при работе с конфиденциальными документами, описать технологии защиты сведений
Исследовать лог файлы веб-сервера	ПК-5 ПК-25	Расчетно-графическая работа	Показывает умения и навыки по восстановлению информации о процессах из дампа ОЗУ, извлечения информации из процесса по дампу ОЗУ

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
3 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и уме-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				ния рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 4	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
5	Расчетно-графическая работа 1	В течение семестра	15 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				все дополнительные вопросы на защите. 10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
Текущий контроль:			55 баллов	
ИТОГО:			55 баллов	

Критерии оценки результатов обучения по дисциплине:
0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);
65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень);
75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень);
85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень).

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Лабораторные работы

Лабораторная работа № 1 Исследование мультимедийного трафика.
В программе Wireshark выполнить:

- Восстановить аудиопоток, переданный через протокол SIP.
- Восстановить видеопоток.

Выполнить отчет о проделанной работе.

Лабораторная работа № 2 Исследование данных передаваемых через протокол TCP.

В программе Wireshark выполнить:

- Восстановить информацию, переданную по протоколу FTP.
- Восстановить информацию, переданную по протоколу SMB2.
- Восстановить информацию, переданную по протоколу HTTP.
- Восстановить информацию, переданную по протоколу SMPT.
- Восстановить информацию, переданную по протоколу POP3.
- Восстановить информацию, переданную по протоколу DNS.
- Восстановить информацию, переданную по протоколу NNTP.
- Восстановить информацию, переданную по протоколу telnet.
- Восстановить информацию, переданную по протоколу LDAP.
- Восстановить информацию, переданную по протоколу HTTPS.

Выполнить отчет о проделанной работе.

Лабораторная работа № 3 Исследование файловых систем операционных систем

- Исследовать структуру файловых систем FAT32, NTFS, Ext4.
- В ручном режиме продемонстрировать удаление и восстановление информации в файловых системах FAT32, NTFS, Ext4.
- Протестировать различное ПО для восстановления файлов (5 шт).
- Протестировать различное ПО для надежного удаления файлов (2 шт).

Выполнить отчет о проделанной работе.

Лабораторная работа № 4 Исследование ОЗУ:

- Восстановить информацию о процессах из дампа ОЗУ.
- Извлечь информацию из процесса по дампу ОЗУ.

Выполнить отчет о проделанной работе.

Задание для расчетно-графической работы

Исследовать лог файлы веб-сервера:

- браузер пользователя;
- персональный межсетевой экран на компьютере пользователя;
- антивирусная программа на компьютере пользователя;
- операционная система пользователя;
- DNS-сервер (резолвер), к которому обращался браузер пользователя перед запросом веб-страницы, а также DNS-сервера (держатели зон), к которым рекурсивно обращался этот резолвер;
- все маршрутизаторы по пути от компьютера пользователя до веб-сервера и до DNS-серверов, а также билинговые системы, на которые эти маршрутизаторы пересылают свою статистику;
- средства защиты (межсетевой экран, система обнаружения атак, антивирус), стоящие перед веб-сервером и вовлеченными DNS-серверами;
- веб-сервер;
- CGI-скрипты, запускаемые веб-сервером;
- Веб-сервера всех счетчиков и рекламных баннеров, расположенных на просматриваемой пользователем веб-странице (как правило, они поддерживаются независимыми провайдерами);

- веб-сервер, на который пользователь уходит по гиперссылке с просматриваемой страницы;
- прокси-сервер (если используется);
- оборудование СОРМ со стороны пользователя и со стороны веб-сервера.

Выполнить отчет о проделанной работе.

Вопросы для защиты лабораторных работ и расчетно-графической работы

1. Информация и документы, считающиеся конфиденциальными.
2. Термин «конфиденциальный, конфиденциальный документ». Конфиденциальное делопроизводство.
3. Признаки конфиденциального документа. Особенности конфиденциального документа.
4. Конфиденциальная информация.
5. Условия отнесения при информации к конфиденциальной. Информация с ограниченным доступом.
6. Классификация КИ предприятия.
7. Сведения, которые не могут являться КИ. Состав и объем сведений, составляющих КИ предприятия
8. Сроки конфиденциальности, порядок защиты и доступа к конфиденциальной информации, правила ее использования.
9. Роль и место конфиденциального делопроизводства в обеспечении защиты конфиденциальной информации, в том числе коммерческой тайны
10. Организация конфиденциального делопроизводства на предприятии
11. Требования нормативных правовых и руководящих документов по организации документационного обеспечения управления предприятием
12. Движение конфиденциальных документов внутри предприятия
13. Создание, регистрация, учет, размножение, обработка, хранение, уничтожение конфиденциальных документов
14. Конфиденциальный документооборот.
15. Отправление конфиденциальных документы.
16. Учет документов с грифом «КИ».
17. Печать документов с грифом «КИ».
18. Регистрация документов с грифом «КИ».
19. Журналы входящих, исходящих и внутренних документов предприятия, содержащих гриф «КИ». Поступающие (входящие) документы с грифом «КИ»
20. Формирование и оформление дел для конфиденциальных документов
21. Разработка инструкций по соблюдению режима конфиденциальности для лиц, допущенных к КИ
22. Использование организационных, технических и иных средств защиты КИ
23. Допуск работника к конфиденциальной информации. Составление «Перечня сведений, содержащих конфиденциальную информацию»
24. Движение (выдача и возврат) документов с грифом «КИ».
25. Защита конфиденциальных документов от подделки: признаки подделки документов и способы их выявления, полная и частичная подделка, способы выявления подделки в документах, технические средства выявления подделок
26. Опишите порядок опечатывания помещения, где хранится информация ограниченного доступа.
27. Опишите порядок опечатывания сейфа(шкафа), где хранится информация ограниченного доступа.
28. Опишите порядок регистрации документов для служебного пользования.

29. Опишите организационные мероприятия по обработке документов для служебного пользования

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
	Изменения внесены в пункт 8.2 Дополнительная литература, страница 7 Добавлен источник №6 1) Цифровая экономика: 2022 : краткий статистический сборник / Г. И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2022 URL:https://publications.hse.ru/pubs/share/direct/553808040.pdf	1