МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО ВГУ)

УТВЕРЖДАЮ
Заведующий кафедрой
алгебры и математических
методов гидродинамики

(Звягин В.Г.)
подпись, расшифровка подписи
25.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.14 Расследование инцидентов информационной безопасности и правонарушений в компьютерной сфере

1. Шифр и наименование специальности:
10.05.04 Информационно-аналитические систем безопасности

2. Профиль специализации: Информационная безопасность финансовых и экономических структур; Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра алгебры и математических методов гидродинамики

6. Составители программы: доцент, к.ф.-м.н., Адамова Римма Сергеевна

7. Рекомендована: НМС математического факультета протокол № 0500-06 от 25.05.2023 г.

8. Учебный год: 2027-2028 **Семестр(ы):** 9

9. **Цели и задачи учебной дисциплины:**
Целью изучения дисциплины является овладение обучающихся теоретическими и практическими основами применения правовой базы, оснований, методов и средств исследования при расследовании компьютерных правонарушений и инцидентов.
Задачи курса:
- знать основные законодательные акты и нормативные документы, связанные с расследованием компьютерных правонарушений и инцидентов;
- уметь использовать законодательные акты и нормативные документы, связанные с осмотром компьютерной техники и поиском, исследованием и изъятием электронной информации в профессиональной деятельности;
- владеть приемами проведения следственных действий применительно к информационным системам.

10. Место учебной дисциплины в структуре ООП:
Блок 1, часть, формируемая участниками образовательных отношений.
Дисциплины учебного плана, с которыми организована взаимосвязь дисциплины рабочей программы: Основы информационной безопасности; Организационное и правовое обеспечение информационной безопасности; Правовое обеспечение профессиональной деятельности.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-4	Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений	ПК-4.1	Анализирует правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицирует факты, события и обстоятельства	Знать: юридические факты, правовые нормы, связи между ними Уметь: анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства Владеть: теоретическими знаниями и навыками работы с юридическими фактами для анализа правоотношений профессиональной деятельности
		ПК-4.2	Обосновывает решения, связанные с реализацией правовых норм в пределах должностных обязанностей	Знать: законодательные акты и нормативные акты в пределах должностных обязанностей Уметь: обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей Владеть: навыками обоснования решений, связанных с должностными обязанностями
		ПК-4.3	Способен искать и анализировать данные из открытых источников с целью обеспечения информационной	Знать: зарубежную и отечественную литературу в предметной области Уметь: искать и анализировать данные из открытых источников с целью обеспечения информационной

			безопасности	безопасности Владеть: источниками информации, навыками работы с литературой, информационными системами
ПК-3	Способен решать типовые задачи обработки и анализа информации в информационно-аналитических системах государственных органов, обеспечивающих национальную безопасность	ПК-3.4	Способен организовывать процесс защиты информации в соответствии с руководящими и методическими документами уполномоченных федеральных органов исполнительной власти	Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти Уметь: организовывать процесс защиты информации в соответствии с руководящими и методическими документами Владеть: навыками организации процесса защиты информации в соответствии с руководящими и методическими документами уполномоченных федеральных органов исполнительной власти

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 4/144.
Форма промежуточной аттестации: экзамен

13. Виды учебной работы

Вид учебной работы	Трудоемкость	
	Всего	По семестрам
		7
Аудиторные занятия	72	72
в том числе: лекции	36	36
практические	36	36
лабораторные	-	-
Самостоятельная работа	36	36
Форма промежуточной аттестации экзамен	36	36
Итого:	144	144

13.1. Содержание разделов дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1	Правовая база расследования компьютерных правонарушений и инцидентов информационной	Понятия компьютерного преступления и инцидента информационной безопасности. Классификация правонарушений в компьютерной сфере	

	безопасности		
2	Основные мероприятия расследования инцидентов информационной безопасности и правонарушений в компьютерной сфере	Возбуждение уголовных дел по преступлениям в сфере высоких технологий. Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации. Осмотр электронных документов. Оперативно-розыскные мероприятия	
3	Организация реагирования	Стандарты и общий цикл управления инцидентами ИБ. Средства обнаружения инцидентов ИБ. Первичное реагирование на инцидент ИБ. Процедура сбора свидетельств инцидента ИБ	
4	Методы и средства исследования компьютерных систем	Выявление элементов инфраструктуры, затронутых инцидентом. Инструменты снятия данных	
2. Практические занятия			
1	Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности	Понятия компьютерного преступления и инцидента информационной безопасности. Классификация правонарушений в компьютерной сфере	
2	Основные мероприятия расследования инцидентов информационной безопасности и правонарушений в компьютерной сфере	Возбуждение уголовных дел по преступлениям в сфере высоких технологий. Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации. Осмотр электронных документов. Оперативно-розыскные мероприятия	
3	Организация реагирования	Стандарты и общий цикл управления инцидентами ИБ. Средства обнаружения инцидентов ИБ. Первичное реагирование на инцидент ИБ. Процедура сбора свидетельств инцидента ИБ	
4	Методы и средства исследования компьютерных систем	Выявление элементов инфраструктуры, затронутых инцидентом. Инструменты снятия данных	

13.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практи-ческие	Лабора-торные	Самостоятель-ная работа	Всего
1	Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности	8	9		9	26
2	Основные мероприятия расследования инцидентов информационной безопасности и правонарушений в	10	9		9	28

	компьютерной сфере					
3	Организация реагирования	7	9		9	25
4	Методы и средства исследования компьютерных систем	12	9		9	30
	Контроль					36
	Итого:	36	36		36	144

14. Методические указания для обучающихся по освоению дисциплины

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, практические занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на практических занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Расследование инцидентов информационной безопасности и правонарушений в компьютерной сфере» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки теорем, разобрать примеры, решенные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.
2. Перед практическим занятием обязательно повторить лекционный материал. После практического занятия еще раз разобрать рассмотренные на этом занятии примеры. Если при решении примеров, возникнут вопросы, обязательно задать на следующем практическом занятии или в присутственный час преподавателю.
3. При подготовке к практическим занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить практические задачи.

Самостоятельная работа обучающихся направлена на самостоятельное освоение всех тем и вопросов учебной дисциплины, предусмотренных программой. Самостоятельная работа является обязательным видом деятельности для каждого обучающегося, ее объем по учебному курсу определяется учебным планом. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся заинтересованное отношение к конкретной проблеме. Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Для успешного и плодотворного обеспечения итогов самостоятельной работы разработаны учебно-методические указания к самостоятельной работе студентов над различными разделами дисциплины.

Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий (практических и теоретических); выполнение контрольных работ; подготовка к практическим занятиям; работа с вопросами для

самопроверки. Все задания, выполняемые студентами самостоятельно, подлежат последующей проверке преподавателем.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Шаньгин, В.Ф. Информационная безопасность и защита информации : учебное пособие / Шаньгин В.Ф. Москва : ДМК-пресс, 2014. 702 с. ISBN 978-5-94074-768-0.
2	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/289
3	Васильева И.Н. Расследование инцидентов информационной безопасности : учебное пособие / И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с. https://www.elibrary.ru/item.asp?id=42343002

б) дополнительная литература:

№ п/п	Источник
4	Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. – М.: ДГСК МВД России, 2017. – 160 с.
5	Кэрриэ Б. Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.
6	Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
7	http://www.lib.vsu.ru/?p=4 - Электронный каталог ЗНБ ВГУ
8	https://ru.wikipedia.org - Википедия
9	http://www.it.ru/ - Информационные технологии

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Васильева И.Н. Расследование инцидентов информационной безопасности : учебное пособие / И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с.
2	Баркалов Ю.М., Нестеровский О.И., Лиходедов Д.Ю. Организационнотехническое обеспечение специальных мероприятий. Метод. рекомендации. – Воронеж: Воронежский институт МВД России, 2016. – 82 с.
3	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете

17. Материально-техническое обеспечение дисциплины:

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ».

Перечень необходимого программного обеспечения: операционная система Windows или Linex, Microsoft, Windows Office, LibreOffice 5, Calc, Math, браузер Mozilla Firefox, Opera или Internet.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория со специализированной мебелью для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации (394018, г. Воронеж, площадь Университетская, д. 1, пом. I)
Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.
При реализации дисциплины с использованием дистанционного образования возможны дополнения материально-технического обеспечения дисциплины

19. Фонд оценочных средств:

Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности	ПК-4, ПК-3	ПК-4.1, ПК-4.2, ПК-4.3, ПК-3.4	Типовые задачи, контрольная работа
2	Основные мероприятия расследования инцидентов информационной безопасности и правонарушений в компьютерной сфере	ПК-4, ПК-3	ПК-4.1, ПК-4.2, ПК-4.3, ПК-3.4	Типовые задачи, контрольная работа
3	Организация реагирования	ПК-4, ПК-3	ПК-4.1, ПК-4.2, ПК-4.3, ПК-3.4	Типовые задачи, контрольная работа
4	Методы и средства исследования компьютерных систем	ПК-4, ПК-3	ПК-4.1, ПК-4.2, ПК-4.3, ПК-3.4	Типовые задачи, контрольная работа
Промежуточная аттестация Форма контроля - экзамен				Перечень вопросов к экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: контрольная работа 1,типовых задач.

Примерный перечень задач для контрольной работы:

Ответить на вопросы:

1. Преступления в сфере информационных технологий включают:

А) распространение вредоносных вирусов
Б) неправильно выключить компьютер
В) кражу номеров кредитных карточек
Г) украсть книжку из библиотеки
Д) взлом паролей
Е) распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

2. По УК РФ преступлениями в сфере компьютерной информации являются:

А) неправомерный доступ к компьютерной информации
Б) Создание, использование и распространение вредоносных компьютерных программ
В) Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации
Г) кража компьютера из офиса
Д) сломать кредитную карточку по неосторожности

3. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в:

А) могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов
Б) серьёзное нарушение работы ЭВМ и их систем
В) несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов
Г) замыкание электросети и электроприборов

4. В каком нормативно правовом акте можно найти санкции за данный вид преступления?

А) Конституция РФ
Б)Конституция РБ
В)Гражданский кодекс РФ
Г) Уголовный кодекс РФ

5. Виды компьютерных преступлений:

А) изменение компьютерных данных
Б) компьютерное мошенничество
В) компьютерное пиратство
Г) прослушивание музыки онлайн

Перечень типовых задач

1.В квартире проживали 4 человека и имелся 1 компьютер. Компьютером 1 января с 19.00 - 21.00 периодически подходили каждый из проживающих. В 20.00 было совершено преступление - неправомерный удаленный доступ к аккаунту в социальной сети посредством подбора пароля. В результате произошло ознакомление с личной информацией, ее копирование, а также рассылка текстовых сообщений от имени потерпевшего. По предварительным данным стало известно, что способ совершения преступления включал в себя следующие действия: использование эксплойта для получения доступа к компьютеру потерпевшего, внедрение в него ВПО, выполняющего поиск документов с паролями, подбор паролей, копирование и пересылка полученной

информации в облачное хранилище. Каждый из проживающих в квартире отрицает свое участие в преступлении, но соглашается с тем, что в период с 19.00 - 21.00 он, как и остальные, мог пользоваться компьютером, в частности, заходить в социальные сети, использовать текстовые и графические редакторы, искать и просматривать информацию в сети Интернет и пр.
Вопросы.
Что способствовало совершению преступления?
Опишите недостающие данные по способу совершения преступления?
Какие средства использовались в данном преступлении?
Какие следы в данной ситуации могут находиться в компьютере, а также какие из них могут персонифицировать преступника?

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

Цель текущего контроля:

Определение уровня сформированности профессиональных компетенций, знаний и навыков деятельности в области знаний, излагаемых в курсе.

Задачи текущего контроля: провести оценивание

1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;

2. степени готовности обучающегося применять теоретические и практические знания и профессионально значимую информацию, сформированности когнитивных умений.

3. приобретенных умений, профессионально значимых для профессиональной деятельности.
Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением контрольных работ.
При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».
В ходе контрольной работы обучающемуся выдается КИМ с теоретическим перечнем заданий и предлагается ответить на вопросы. За каждый правильный ответ обучающийся получает 1 балл. Если студент набирает 3 баллов, он получает оценку «удовлетворительно», 4 балла – «хорошо», 5 баллов – «отлично». В ходе выполнения заданий нельзя пользоваться конспектами аудиторных занятий, мобильным телефоном и другой техникой, ограничение по времени 1 час 30 минут.
Если текущая аттестация проводится в дистанционном формате, то у обучающийся обязательно должен иметь компьютер, микрофон, камеру. Если у обучающегося отсутствует необходимое оборудование, то он обязан сообщить преподавателю об этом за 3 суток. На контрольную работу в дистанционном режиме отводится ограничение по времени 1 час 45 минут.
При решении типовых задач используется следующий критерий оценивания:
«Отлично»: Студентом задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом.
«Хорошо»: Студентом задание решено с подсказкой преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение

решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
«Удовлетворительно»: Студентом задание решено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задание решено не полностью или в общем виде.
«Неудовлетворительно»: Студентом задание не решено.

20.2. Промежуточная аттестация

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Расследование инцидентов информационной безопасности и правонарушений в компьютерной сфере» проводится в форме экзамена.
Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося могут быть учтены при проведении промежуточной аттестации (как среднее арифметическое оценок за контрольную работу и типовую задачу). При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.
При проведении экзамена учитываются ответы на задания билета.

Примерный перечень вопросов:

1	Понятия компьютерного преступления и инцидента информационной безопасности
2	Понятие инцидента информационной безопасности
3	Классификация правонарушений в компьютерной сфере
4	Криминалистическая характеристика правонарушений в компьютерной сфере
5	Возбуждение уголовных дел по преступлениям в сфере высоких технологий
6	Привлечение к расследованию специалистов
7	Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации (часть 1)
8	Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации (часть 2)
9	Осмотр электронных документов
10	Перехват и исследование сетевого трафика
11	Использование кейлогеров
12	Поиск информации в открытых источниках
13	Определение принадлежности IP адресов
14	Определение принадлежности доменных имен. Определение принадлежности адреса электронной почты
15	Назначение компьютерной экспертизы
16	Стандарты и общий цикл управления инцидентами ИБ
17	Средства обнаружения инцидентов ИБ
18	Правовые основания использование данных мониторинга и DLP-систем

19	Первичное реагирование на инцидент ИБ
20	Процедура сбора свидетельств инцидента ИБ
21	Группа реагирования на инциденты
22	Выявление элементов инфраструктуры, затронутых инцидентом
23	Инструменты снятия данных

Для оценивания результатов обучения на экзамене используются следующие **показатели:**

1) знание теоретических основ;
2) умение решать задачи
3) умения применять знания в профессиональной сфере;
4) успешное прохождение текущей аттестации.

Для оценивания результатов экзамена используется ***шкала:*** «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие обучающимся всем перечисленным показателям по каждому из вопросов контрольно-измерительного материала. Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, применять теоретические знания для решения практических задач в области курса, студент умеет работать с различными источниками научной информации, грамотно и правильно представляет свои результаты, правильно отвечает на вопросы КИМ	Повышенный уровень	Отлично
Несоответствие ответа обучающегося одному из перечисленных выше показателей (к одному из вопросов контрольно-измерительного материала) и правильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым двум из перечисленных показателей (либо двум к одному вопросу, либо по одному к каждому вопросу контрольно-измерительного материала) и правильные ответы на два дополнительных вопроса в пределах программы.	Базовый уровень	Хорошо
Несоответствие ответа обучающегося любым двум из перечисленных показателей и неправильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым трем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	Пороговый уровень	Удовлетвори-тельно
Несоответствие ответа обучающегося любым из перечисленных показателей (в различных комбинациях по отношению к вопросам	–	Неудовлетвори тельно

контрольно-измерительного материала).		

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Киберпреступление-это…

а) любое деяние, в котором инструментом, целью или местом преступных действий являются компьютерные системы

б) возможность получения информации и её использования

в) доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

г) совокупность правил, регламентирующих права доступа субъектов доступа к объектам.

Ответ: а)

2. Доступ к информации-это…

а) любое деяние, в котором инструментом, целью или местом преступных действий являются компьютерные системы

б) возможность получения информации и её использования

в) доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

г) совокупность правил, регламентирующих права доступа субъектов доступа к объектам.

Ответ: б)

3. Несанкционированный доступ-это…

а) любое деяние, в котором инструментом, целью или местом преступных действий являются компьютерные системы

б) возможность получения информации и её использования

в) доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

г) совокупность правил, регламентирующих права доступа субъектов доступа к объектам.

Ответ: в)

4. Правила разграничения доступа-это…

а) любое деяние, в котором инструментом, целью или местом преступных действий являются компьютерные системы

б) возможность получения информации и её использования

в) доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

г) совокупность правил, регламентирующих права доступа субъектов доступа к объектам.

Ответ: г)

5. Вредоносное программное обеспечение-это …

а) компьютерная программа, предназначенная для нанесения вреда (ущерба) владельцу (пользователю) компьютерное информации, хранящейся на средствах вычислительной техники, путём ей несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на СВТ средств защиты, или для получения доступа к вычислительным ресурсом самого СВТ с целью их несанкционированного использования

б) факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки

в) объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов

г) информационная система, информационно-телекоммутативные сети, автоматизированные системы управления субъектов КИИ

Ответ: а)

6. Преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем являются: несанкционированный доступ, незаконное получение данных, незаконный перехват, искажение информации, искажение …

Ответ: системы

7. Преступлениями, связанными с правами собственности и товарными знаками, являются: преступления, связанные с нарушенияем авторских и смежных прав; преступления, связанные с … знаками

Ответ: товарными

8. Преступлениями, связанными с применением компьютерной техники, являются: компьютерное мошенничество, подлог, кража…, злоупотребление устройствами.

Ответ: идентичности

9. К комбинированным преступлениям относятся использование сети Интернет в террористических целях, кибервойны, фишинг, отмывание денег с использование компьютерных…

Ответ: технологий

10. Система действий по подготовке, совершения и сокрытию правонарушения называется способом совершения…

Ответ: преступления

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

3) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).

Программа рекомендована НМС математического факультета протокол № 0500-06

от 25.05.2023 г.