Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 16:08:31
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Компьютерная криминалистика»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Преподаватель  /Г.Ф. Шипулин/

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 4
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 5
3.3 Содержание дисциплины 6
3.4 Тематика семинарских/практических и лабораторных занятий 6
3.5 Тематика курсовых проектов (курсовых работ) 6
4 Учебно-методическое и информационное обеспечение 7
4.1 Нормативные документы и ГОСТы 7
4.2 Основная литература 7
4.3 Дополнительная литература 7
4.4 Электронные образовательные ресурсы 7
4.5 Лицензионное и свободно распространяемое программное обеспечение 8
4.6 Современные профессиональные базы данных и информационные справочные системы 8
5 Материально-техническое обеспечение 8
6 Методические рекомендации 8
6.1 Методические рекомендации для преподавателя по организации обучения 8
6.2 Методические указания для обучающихся по освоению дисциплины 8
7 Фонд оценочных средств 9
7.1 Методы контроля и оценивания результатов обучения 9
7.2 Шкала и критерии оценивания результатов обучения 9
7.3 Оценочные средства 10

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью преподавания дисциплины является формирование у студентов знаний в области компьютерной криминалистики, сбора и анализа цифровых доказательств.
Задачи преподавания дисциплины:

- изучение этапов, методов и средств проведения компьютерно-технических экспертиз;
- освоение способов и методов средств сбора цифровых доказательств;
- освоение методов организации и управления деятельности служб защиты информации на предприятии.

В результате освоения дисциплины «Компьютерная криминалистика» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:
знать:
- принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);
уметь:
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;
владеть:
- методами организации и управления деятельность служб защиты информации на предприятии.

Обучение по дисциплине «Компьютерная криминалистика» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. Владеет методами организации и управления деятельность служб защиты информации на предприятии.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерная криминалистика» относится к числу элективных профессиональных учебных дисциплин части, формируемой участниками образовательных отношений (Б1.2. ЭД.3) основной образовательной программы (Б1.2.ЭД.3.1).
Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Мониторинг событий и управление инцидентами (SIEM)», «Основы управления информационной безопасностью».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, т.е. 144 часов (лекции – 4 часов, лабораторные занятия – 72 часа, самостоятельная работа - 72 часа, форма контроля – экзамен) в 7 семестре.
Структура и содержание дисциплины «Компьютерная криминалистика» по срокам и видам работы отражены в приложении

3.1Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			7	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**72**	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		Экзамен	
	Итого	**144**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1.						
1.1	Тема 1. Введение в компьютерную криминалистику.	8					4
1.2	Тема 2. Компьютерная форензика.	72			36		36
1.3	Тема 3. Сетевая форензика.	64			36		32
	Итого	**144**	**4**		**72**		**72**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3. Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1	
1.1	Введение в компьютерную криминалистику.	Компьютерная криминалистика: определение, классификация, цели и задачи, разбор практических кейсов. Компьютерная экспертиза: определение, классификация, этапы проведения. СОРМ.
1.2	Компьютерная форензика.	Устройство hdd, ssd и flash накопителей. Способы и средства анализа файловых систем, восстановление данных, метаданные файлов. Программные и аппаратные средства копирования носителей информации. RAM-память: устройство, инструментальные средства копирования и анализа. Анализ систем под управлением ОС Windows. Анализ систем под управлением ОС Linux.
1.3	Сетевая форензика.	Межсетевые экраны, IPS, IDS, SIEM-решения. Аудит событий ОС Linux, Windows. Методы и способы выявления сетевых атак на основе анализа трафика.

3.4Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение лабораторной работы №1 по теме 2	36
2	Выполнение лабораторной работы №2 по теме 3	36
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.05.03 «Информационная безопасность автоматизированных систем».

4.2 Основная литература

1. Компьютерная криминалистика : учебное пособие / составители И. А. Калмыков, В. С. Пелешенко. — Ставрополь : СКФУ, 2017. — 84 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155227 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.
2. Островская, С. Криминалистика компьютерной памяти на практике. Как эффективно анализировать оперативную память / С. Островская, О. Скулкин ; редактор С. Островская ; перевод с английского А. А. Слинкина. — Москва : ДМК Пресс, 2023. — ISBN 978-5-93700-157-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/314951 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.
3. Ваценко, А.А. Обзор техник компьютерной криминалистики / А. А. Ваценко // Бюллетень науки и практики. — 2020. — № 6. — С. 167-174. — ISSN 2414-2948. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/312872 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.

4.3 Дополнительная литература

1. Маркагич, М.С. КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА В ОБЛАСТИ ЭЛЕКТРОННОЙ ПОЧТЫ / М.С. Маркагич // Vojnotehnicki glasnik / Military Technical Courier / Военно-технический вестник. — 2013. — № 3. — С. 113-121. — ISSN 0042-8469. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/296235 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.
2. Ваценко, А.А. Обзор техник компьютерной криминалистики / А. А. Ваценко // Бюллетень науки и практики. — 2020. — № 6. — С. 167-174. — ISSN 2414-2948. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/312872 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.
3. Каминский, М.К. ОБРАЗОВАНИЕ И ОБУЧЕНИЕ В КРИМИНАЛИСТИКЕ: ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ УЧЕБНОГО КУРСА / М. К. Каминский, А. М. Каминский // Вестник Удмуртского университета. Серия Экономика и право.

4.4 Электронные образовательные ресурсы

1. ЭОР «Основы форензики» [Электронный ресурс] — URL: https://online.mospolytech.ru/course/view.php?id=10983 (дата обращения: 18.02.2023).

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Дистрибутив ОС Kali Linux
4. Дистрибутив ОС Windows Server 2012/2016
5. Дистрибутив ОС Windows 7, 10

4.6 Современные профессиональные базы данных и информационные справочные системы

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопрос для проведения экзамена по дисциплине:
1. Форензика: определение, классификация, цели и задачи.
2. Компьютерная экспертиза: определение, классификация, используемое ПО.
3. Виды и архитектура СОРМ.
4. Устройство hdd, ssd и flash накопителей.
5. Способы и средства анализа файловых систем.
6. Программные и аппаратные средства копирования носителей информации.
7. RAM-память: устройство, инструментальные средства копирования.
8. Анализ систем под управлением ОС Windows.
9. Анализ систем под управлением ОС Linux.
10. Межсетевые экраны.
11. Системы обнаружения и предотвращения вторжений.
12. SIEM-системы.
13. Аудит событий ОС Linux.
14. Аудит событий ОС Windows.
15. Методы и способы выявления сетевых атак на основе анализа трафика.
16. Способы и средства восстановление данных.
17. Способы и средства извлечения и анализа метаданные файлов.
18. Этапы проведения компьютерных экспертиз.
19. RAM-память: устройство, инструментальные средства анализа.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Компьютерная криминалистика
Бакалавры. Курс 4, семестр 1

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Системы обнаружения и предотвращения вторжений.
2. RAM-память: устройство, инструментальные средства анализа.

Преподаватель _____ / Шипулин Г.Ф. /