МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кузбасский гуманитарно-педагогический институт

Факультет истории и права
Кафедра уголовно-правовых дисциплин

УТВЕРЖДАЮ
Декан ФИП

Л.А. Юрьева
«17» февраля 2025 г.

Рабочая программа дисциплины

К.М.02.07 Информационные технологии и информационная безопасность
Код, название дисциплины

Направление подготовки

40.04.01 Юриспруденция

Направленность (профиль) программы

«Юрист в сфере правосудия по уголовным делам»

Программа магистратуры

Квалификация выпускника
магистр

Формы обучения
очная, заочная

Год набора 2025

Новокузнецк 2025

Лист внесения изменений
в РПД *К.М.02.07 Информационные технологии и информационная безопасность*

Сведения об утверждении:
утверждена Ученым советом факультета истории и права
(протокол Ученого совета факультета № 7 от 17.02.2025 г.)

для ОПОП 2025 года набора на 2025–2026 учебный год
по направлению подготовки 40.04.01 Юриспруденция
направленность (профиль) программы «Юрист в сфере правосудия по уголовным делам»

Одобрена на заседании методической комиссии факультета истории и права
(протокол методической комиссии факультета № 4 от 10.02.2025 г.)

Одобрена на заседании обеспечивающей кафедры информатики и вычислительной техники им. Буторина В.К.

Оглавление

1 Цель дисциплины

В результате освоения дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы магистратуры (далее – ОПОП): ОПК-7.

Содержание компетенций как планируемых результатов обучения по дисциплине – см. таблицы 1 и 2.

1.1 Формируемые компетенции

Таблица 1 – Формируемые дисциплиной компетенции

Наименование вида компетенции *(универсальная, общепрофессиональная, профессиональная)*	Наименование категории (группы) компетенций	Код и название компетенции
Общепрофессиональная	Информационные технологии	ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК 7.1. Имеет представление об информационных технологиях и правовых базах данных, применяемых и используемых для решения задач профессиональной деятельности ОПК-7.2. Способен искать, создавать, анализировать информацию в цифровой среде для решения задач профессиональной деятельности с учетом требований информационной безопасности	Информационные технологии и информационная безопасность Преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК 7.1. Имеет представление об информационных технологиях и правовых базах данных, применяемых и используемых для решения задач профессиональной деятельности ОПК-7.2. Способен искать, создавать, анализировать информацию в цифровой среде для решения задач профессиональной деятельности с учетом требований информационной безопасности	**знать** принципы работы правовых баз данных, справочно-информационных систем; требования информационной безопасности при работе с данными; методы анализа и сбора информации в цифровой среде **уметь** осуществлять поиск и мониторинг данных в открытых источниках и справочных правовых системах; собирать данные о состоянии компьютерной системы; определять факт нарушения информационной безопасности в цифровой среде **владеть** навыками работы с правовыми базами данных и справочно-правовыми системами; навыками определения категории информации, соблюдения правил работы с персональными данными и другими видами защищаемой информации

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 4 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения		
	ОФО	ОЗФО	ЗФО
1 Общая трудоемкость дисциплины	180	–	180
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	28	–	12
Аудиторная работа (всего):	28	–	12
в том числе:		–	
лекции	12	–	6
практические занятия, семинары	16	–	6
практикумы	–	–	–
лабораторные работы	–	–	–

в интерактивной форме	–	–	–
в электронной форме	–	–	–
Внеаудиторная работа (всего):	–	–	–
в том числе, индивидуальная работа обучающихся с преподавателем	–	–	–
подготовка курсовой работы / контактная работа	–	–	–
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)	–	–	–
творческая работа (эссе)	–	–	–
3 Самостоятельная работа обучающихся (всего)	116	–	159
4 Промежуточная аттестация обучающегося	экзамен (36)	–	экзамен (9)

3 Учебно-тематический план и содержание дисциплины

3.1 Учебно-тематический план

Таблица 5 – Учебно-тематический план *очной* формы обучения

№ п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.) ОФО			Формы текущего контроля и промежуточной аттестации успеваемости
			Аудиторные занятия		СРС	
			лекц.	практ.		
1	Правовые базы данных	44	4	5	35	Тестирование
2	Информационная безопасность в профессиональной сфере	52	4	6	42	ИДЗ № 1-2
3	Основы компьютерной криминалистики	48	4	5	39	Тестирование
	Промежуточная аттестация **(36 час.)**					Экзамен
	Всего:	**180**	**12**	**16**	**116**	

Таблица 5.1 – Учебно-тематический план *заочной* формы обучения

№ п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.) ЗФО			Формы текущего контроля и промежуточной аттестации успеваемости
			Аудиторные занятия		СРС	
			лекц.	практ.		
1	Правовые базы данных	54	2	2	50	Тестирование
2	Информационная безопасность в профессиональной сфере	60	2	2	56	ИДЗ № 1-2
3	Основы компьютерной криминалистики	57	2	2	53	Тестирование
	Промежуточная аттестация **(9 час.)**					Экзамен
	Всего:	**180**	**6**	**6**	**159**	

3.2 Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Содержание лекционного курса	
1	Правовые базы данных	Понятие каталога, базы данных, хранилища данных. Понятие справочно-правовых информационных систем (СПС). Рынок СПС. Поисковая машина: принципы работы, индексация, язык поисковых запросов. Правовые порталы и сервисы
2	Основы информационной безопасности	Термины и определения. Подходы и концепции в обеспечении информационной безопасности. Требования законодательства, нормативно-правовые основы, регуляторы информационной безопасности. ФЗ «Об информации, информационных технологиях и о защите информации», отечественные и международные стандарты в области защиты информации, руководящие документы ФСТЭК.
3	Меры защиты информации. Прикладная безопасность конечных машин	Направления защиты информации. Средства и способы защиты информации. Классификации угроз уязвимости. Объекты защиты. Правовые средства обеспечения безопасности информации. Организационное обеспечение информационной безопасности РФ. Организационно-правовые проблемы международной информационной безопасности. Правовые режимы обеспечения безопасности информации ограниченного доступа. Особенности организационно-правового обеспечения защиты информационных систем. Юридическая ответственность за правонарушения в информационной сфере. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения: классификация вредоносных программ, защита от вредоносных программ, методы тестирования программного обеспечения на его защищенность, методы защиты программ от несанкционированного исследования и копирования.
4	Теория безопасности передачи данных	Схемы электронной подписи. Схемы построения хэш-функций. Схемы построения псевдослучайных генераторов. Протоколы аутентификации. Протоколы распределения ключей. Разновидности протоколов электронной подписи. Протоколы финансовой криптографии. Основы сетевой безопасности. Виды сетевых атак. Средства безопасности сети
5	Основные понятия компьютерной криминалистики	Компьютерная криминалистика (Форензика). Основные задачи компьютерной криминалистики. Научные методы, применяемые в компьютерной криминалистики и их особенности. Сценарии компьютерно-технических экспертиз. Компьютерная контр–криминалистика Сбор

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
		цифровых доказательств. Источники криминалистически значимой компьютерной информации. Сценарии.
6	Реагирование на инциденты в информационной безопасности	Понятие инцидента. Управление Инцидентами ИБ. Реагирование на инциденты Понятие риска в сфере ИБ. Управление рисками. Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построение систем защиты информации. Методики и программные продукты для оценки рисков.
	Содержание практических занятий	
	Правовые базы данных	
1	Практическая работа № 1. Использование справочно-правовых систем для получения и анализа актуальной информации при организации правоохранительной деятельности	Организация поиска в справочно-правовой системе «Консультант Плюс» с использованием Карточки поиска. Отбор и фильтрация списков документов. Работа с тематическим классификатором справочно-правовой системы. Поиск и анализ судебной практики в справочно-правовой системе. Создание подборок и списков отслеживания нормативно-правовых актов.
2	Практическая работа № 2. Поиск и анализ актуальных нормативно-правовых актов с использованием сетевых ресурсов и порталов.	Официальный интернет-портал правовой информации pravo.gov.ru. Создание запросов и подборок в интегрированном банке «Законодательство России» Государственная информационная система «Правосудие» sudrf.ru. Поиск судебных актов. Ресурсы судебной власти. Судебная практика. Статистические данные. Интернет ресурсы субъектов РФ. Официальные ресурсы президента и правительства. Официальные ресурсы министерств, служб и агентств РФ. Использование интернет-ресурсов для поиска и анализа информации. Единые реестры. Аналитические порталы, отчетность, статистические данные.
	Информационная безопасность в профессиональной сфере	
3	Практическая работа № 3. Построение модели угроз и уязвимостей и модели нарушителя	Определение защищаемой информации на объекте. Определение источника информации, направления защиты информации. Определение объекта защиты. Составление модели нарушителя: тип, вид и потенциал, цели, способы реализации Построение модели доступа к информации, источнику информации
4	Практическая работа № 4. Техническая защита информации. Моделирование кабинета руководителя организации как объекта защиты	Составление характеристики информации, защищаемой в помещении – виды информации, источники информации и т.д. (с точки зрения инженерно-технической защиты). Построение плана кабинета, оформление результатов обследования помещения. Планирование системы технической защиты информации

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
5	Практическая работа № 5. Правовая защита информации. Решение практических задач	Выявление нарушений информационной безопасности.
6	Практическая работа № 6. Цифровая гигиена и защита личной информации	Выявление вредоносного ПО. Выявление фишинга. Виды мошенничества в сети.
	Основы компьютерной криминалистики	
7	Практическая работа № 7. Сценарии сбора доказательств	Сценарии компьютерно-технических экспертиз. Сценарии сбора цифровых доказательств.
	Промежуточная аттестация – *экзамен*	

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 7.

Таблица 7 – Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы (мин.-макс.)
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**80**	Практические работы	**3 балла** (выполнено 51–85% заданий) **5 баллов** (выполнено 86–100% заданий)	21–35
		Тест	**5 баллов** (выполнено 51– 85% заданий) **10 баллов** (выполнено 86–100% заданий)	10–20
		Индивидуальное задание	**5 баллов** (выполнено 51–85% заданий) **13 баллов** (выполнено 86–100% заданий)	10–26
Итого по текущей работе в семестре				41–80
Промежуточная аттестация	**20**	Ответ на теоретический вопрос 1	**1 балл** (пороговое значение) **2 балла** (максимальное значение)	1–2
		Ответ на теоретический вопрос 2	**1 балл** (пороговое значение) **2 балла** (максимальное значение)	1–2
		Выполнение практического задания 1	**5 баллов** (пороговое значение) **8 баллов** (максимальное значение)	5–8
		Выполнение практического задания 2	**5 баллов** (пороговое значение) **8 баллов** (максимальное значение)	5–8
Итого по промежуточной аттестации				10–20 б.
Суммарная оценка по дисциплине: сумма баллов текущей и промежуточной аттестации				51–100 б.

Для оценивания результатов учебной работы студентов заочной формы обучения преподавателем может применяться поправочный коэффициент с учетом количества оценочных мероприятий.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале

и в буквенном эквиваленте (таблица 7.1).

Таблица 7.1 – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки

Сумма набранных баллов	Уровни освоения дисциплины и компетенций	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86–100	Продвинутый	5	отлично	Зачтено
66–85	Повышенный	4	хорошо	
51–65	Пороговый	3	удовлетворительно	
0–50	Первый	2	неудовлетворительно	Не зачтено

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины

5.1 Учебная литература

Основная учебная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544290 (дата обращения: 20.01.2025).

2. Информационные технологии в юридической деятельности : учебник и практикум для вузов / В. Д. Элькин [и др.] ; под редакцией В. Д. Элькина. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 472 с. – (Высшее образование). – ISBN 978-5-534-12733-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/535552 (дата обращения: 20.01.2025).

Дополнительная учебная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 277 с. – (Высшее образование). – ISBN 978-5-534-16450-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544029 (дата обращения: 20.01.2025).

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 327 с. – (Высшее образование). – ISBN 978-5-534-16772-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/542739 (дата обращения: 20.01.2025).

3. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 357 с. – (Высшее образование). – ISBN 978-5-534-19108-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/555950 (дата обращения: 20.01.2025).

4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Издательство Юрайт, 2024. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/543351 (дата обращения: 20.01.2025).

5. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. – 7-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 427 с. –

(Высшее образование). – ISBN 978-5-534-18043-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/535625 (дата обращения: 20.01.2025).

5.2 Материально-техническое и программное обеспечение дисциплины

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений
1	2
410 Учебная аудитория (мультимедийная) для проведения: – занятий лекционного типа; – занятий семинарского (практического) типа; – групповых и индивидуальных консультаций; – текущего контроля и промежуточной аттестации; – государственной итоговой аттестации. **Специализированная (учебная) мебель**: доска меловая, кафедра, моноблоки аудиторные. **Оборудование для презентации учебного материала:** *стационарное* – компьютер, экран, проектор, акустическая система. Количество посадочных мест – 46. **Используемое программное обеспечение**: LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС**.	654079, Кемеровская область, г. Новокузнецк, Центральный район, просп. Металлургов, дом № 19
502 Компьютерный класс / Лаборатория компьютерного моделирования. Учебная аудитория (мультимедийная) для проведения: – занятий лекционного типа; – занятий семинарского (практического) типа; – занятий лабораторного типа; – учебных и производственных практик; – курсового проектирования (выполнения курсовых работ); – групповых и индивидуальных консультаций; – самостоятельной работы; – текущего контроля и промежуточной аттестации; – государственной итоговой аттестации. **Специализированная (учебная) мебель**: доска меловая, столы компьютерные, стулья. **Оборудование для презентации учебного материала:** *стационарное* – компьютер, экран, проектор, наушники. **Лабораторное оборудование**: *стационарное* – компьютеры для обучающихся (20 шт.). Количество посадочных мест – 20. **Используемое программное обеспечение**: LibreOffice (свободно распространяемое ПО), AUTOCAD (Коробочная лицензия №	654079, Кемеровская область, г. Новокузнецк, Центральный район, просп. Металлургов, дом № 19

0730450), AlteraQuartusPrimeLite (бесплатное ПО), AutoLOGIC (разработка составителя Шехтмана), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Java (бесплатная версия), MASM32 (свободно распространяемое ПО), ModelSimAltera (бесплатная версия), Mpich 2 (свободно распространяемое ПО), Netbeans IDE 7.0.1 для Firefox (свободно распространяемое ПО), OpenProject (бесплатная версия), Opera 12 (свободно распространяемое ПО), Oracle VM VirtualBox (бесплатная версия), Paint.NET (свободно распространяемое ПО), PostgreSQL (свободно распространяемое ПО), Qt (свободно распространяемое ПО), Eclipse (свободно распространяемое ПО), Quick-TUTOR (разработка составителя), Scilab (свободно распространяемое ПО), SWI-Prolog (свободно распространяемое ПО), TexasInstruments TINA-TI (бесплатная версия), UML-диаграммы (бесплатная версия), Консультант Плюс (отечественное ПО, договор об инфо поддержке 1.04.2007), OMRON CX-One LITE v4.26 (демонстрационная версия), пакет программирования панелей оператора OMRON серии NBNB-Designer v1.20 (демонстрационная версия), ППП nanoCAD, nanoCADЭлектро, nanoCAD СКС, nanoCAD Схемы (отечественное ПО, демонстрационная версия), ППП GENESIS 32 (демонстрационная версия), GPSS WorldStudentEdition (учебная версия), XAMPP (свободно распространяемое ПО), Denwer (свободно распространяемое ПО), T-FlexCAD (учебная версия), 3ds MaxDesign (Коробочная лицензия № 0730450), Галактика (отечественное ПО, договор 2012/339 от 04.12.2012, Акт 000017 27.02.2013), Среда статистических вычислений Rv.4.0.2 (свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	

5.3 Современные профессиональные базы данных и информационные справочные системы

CITForum.ru – on-line библиотека свободно доступных материалов по информационным технологиям на русском языке – http://citforum.ru

Базы данных и аналитические публикации на портале «Университетская информационная система Россия», режим доступа: https://uisrussia.msu.ru/

Официальный интернет-портал правовой информации, режим доступа – http://pravo.gov.ru/

Государственная информационная система «Правосудие», режим доступа – https://sudrf.ru/

6 Иные сведения и (или) материалы

6.1 Примерные темы письменных учебных работ

Индивидуальное задание № 1

Разработать регламент информационной безопасности предприятия (политику безопасности).

Регламент должен включать:

- назначение и правовая основа документа;
- объекты защиты (информационные ресурсы, процессы обработки, инфраструктуру)
- структура, состав и размещение основных объектов защиты, информационные связи
- категории информационных ресурсов, подлежащих защите
- цели и задачи защиты
- пути реализации различных угроз безопасности информации
- регламентация доступа в помещения
- регламентация допуска сотрудников к использованию информационных ресурсов
- регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов
- обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов
- безопасность персональных данных

Индивидуальное задание №2

1. Постройте модели угроз информационной безопасности для объекта
2. Оцените риски информационной безопасности
3. Составьте требования защиты информационной безопасности на базовом уровне
4. Рассчитайте экономическое обоснование
5. Составьте оценку производительности

6.2 Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 9 – Типовые (примерные) контрольные вопросы и задания

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания
Правовые базы данных	1. Настройка контроля и мониторинга нормативных документов в справочно-правовых системах 2. Функциональные возможности правового портала 3. Сервисы электронного суда	1. Найти нормативные акты по известным реквизитам 2. Определить последние принятые изменения в нормативном документе 3. Составить подборку документов по теме 4. Найти и заполнить форму заявления на выдачу подотчетных денег 5. Составить подборку прецедентов по тематике
Основы информационной безопасности	4. Классификация средств и способов защиты информации 5. Защищаемая информация. 6. Объекты защиты 7. Регламентирующие нормативные акты 8. Международные стандарты в области защиты информации 9. Правовые средства защиты информации 10. Информация ограниченного доступа. Правовые режимы обеспечения безопасности 12. Юридическая ответственность за правонарушения	6. Классифицировать защищаемую информацию 7. Определить объекты защиты на предприятии 8. Определить юридическую ответственность за несанкционированный доступ к государственной тайне 9. Определить юридическую ответственность за распространение вредоносного ПО 10. Определить организационные меры защиты для ИСПДн отдела кадров

	13. Организационное обеспечение безопасности	
Основы компьютерной криминалистики	14. Компьютерная криминалистика 15. Компьютерная контр-криминалистика 16. Сценарии сбора доказательств 17. Источники криминалистически значимой компьютерной информации.	

Составитель (и): Штейнбрехер О.А., канд. техн. наук, доцент кафедры ИВТ им. Буторина В.К.

(*фамилия, инициалы и должность преподавателя (ей)*)