Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Северо-Осетинский государственный университет имени Коста Левановича Хетагурова»

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# **«Профилактика преступлений в сфере компьютерной информации»**

Направление подготовки:
***40.04.01 «Юриспруденция»***

Программа «Уголовное право и криминология»

Квалификация (степень) выпускника – магистр

Форма обучения – очная, заочная

Год начала подготовки – 2026

Утверждена в составе ОПОП.

Составитель зав. кафедрой уголовно-правовых дисциплин, к.ю.н., доцент. Л.Х. Караева

Владикавказ 2026

## 1. Структура, и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы 108 часов.

| | ОФО | ЗФО |
|---|---|---|
| Курс | 1 | 1 |
| Семестр | 1 | - |
| Лекции | - | - |
| Практические занятия | - | - |
| Лабораторные занятия | 18 | 8 |
| Консультации | - | - |
| Итого аудиторных занятий | 18 | 8 |
| Самостоятельная работа | 90 | 100 |
| Курсовая работа | - | - |
| экзамен | - | - |
| Зачет с оценкой | 1 семестр | 1 курс |
| Общее количество часов | 108 | 108 |

## 2. Цели изучения дисциплины

Целями освоения учебной дисциплины «Профилактика преступлений в сфере компьютерной информации» является: формирование у студентов магистратуры научного мировоззрения, знаний концептуальных основ уголовного права, умений и навыков по выявлению актуальных проблем уголовного права на законодательном, теоретическом и правоприменительном уровнях, а также способности находить нравственно приемлемые, научно и логически обоснованные пути их решения.

## 3. Место дисциплины в структуре ОПОП:

Дисциплина «Профилактика преступлений в сфере компьютерной информации» Б1.В.ДВ.06.02 Блок 1. Часть, формируемая участниками образовательных отношений. Дисциплина «Профилактика преступлений в сфере компьютерной информации» дает возможность углубить комплекс знаний в области уголовного права, позволяющих самостоятельно решать вопросы правового характера.

Для успешного освоения дисциплины студент должен иметь базовую подготовку по уголовному праву.

## 4. Требования к результатам освоения дисциплины

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

Способен применять нормативные правовые акты в конкретных областях (сферах) деятельности (ПК-2).

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

| ***Код компетенции Формулировка компетенции*** | ***Код и наименование индикатора достижения компетенции*** | ***Результаты обучения*** |
|---|---|---|
| **ПК-2** Способен применять нормативные правовые акты в конкретных областях (сферах) деятельности. | ИПК 2.1 Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права<br>ИПК 2.2 Понимает особенности различных форм реализации права<br>ИПК 2.3 Устанавливает фактические обстоятельства, имеющие юридическое значение<br>ИПК 2.4 Определяет характер правоотношения и подлежащие применению нормы материального и процессуального права | **Знать:**<br>-нормы законодательства, регулирующие сферу деятельности;<br>- соответствующую норму права, толковать и применять ее к конкретной правовой ситуации;<br>- принципы формирования системы законодательства Российской Федерации и свободно ориентироваться в отраслевом |

| | | |
|---|---|---|
| | ИПК 2.5 Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права | законодательстве соответствующего профиля.<br>**Уметь:**<br>-толковать правовые нормы, составлять проекты документов;<br>- - принимать решения в соответствии с законодательством Российской Федерации при оценке конкретных жизненных обстоятельств;<br>- определять соответствующие нормы права, позволяющие принять правильное решение и совершить юридические действия;<br>- обосновать последствия принятых решений в соответствии с положениями нормативно-правовых актов.<br>**Владеть**:<br>- навыками работы с правовыми базами данных;<br>- навыками четко и ясно определять, и формулировать цели, задачи и средства совершения юридических действий;<br>- навыками оформления результатов принятого решения в соответствии с требованием норм отраслевого. |

## 5. Содержание и учебно-методическая карта дисциплины

### 5.1. Очная форма обучения

| № недели | Наименование тем (вопросов), изучаемых по данной дисциплине | Занятия | | Самостоятельная работа обучающихся | | Формы контроля | Литература |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаб. | Содержание | Часы | | |
| 1. | **Тема 1. Уголовно-правовая природа преступлений в сфере обращения цифровой информации**<br>1. Понятие цифровой информации.<br>2. Понятие преступлений в сфере обращения цифровой информации.<br>3. Феномен безопасной компьютерной атаки. | - | 2 | 1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации.<br>2. Латентность преступлений в сфере компьютерной информации.<br>3. Оценка общественной опасности и распространенности преступлений в глобальных компьютерных сетях. | 10 | Устный опрос Проверка практических навыков. | [1] -[6] |
| 2. | **Тема 2. Научно-технический прогресс и его последствия (побочные эффекты)**<br>1. Научно-техническая революция и социальное развитие.<br>2. Человек – компьютер – преступление.<br>3. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны. | - | 2 | Цифровизация социального пространства как непосредственное влияние на трансформацию права. Внесение дополнений в законодательство, направленные на создание эффективных правовых средств противодействия новым формам криминальной деятельности. Современные цифровые платформы, используемые в уголовном праве, в теории и на практике. Определение понятия «цифровая личность». Преимущества и недостатки создания «цифрового закона». | 10 | Устный опрос Проверка практических навыков. | [1] -[6] |
| 3. | **Тема 3. Основные законы и понятия современного информационного оборота**<br>1. Значение информации в жизни | - | 2 | Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации | 12 | Устный опрос Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | социума.<br>2. Правовое понятие и сущность компьютерной информации.<br>3. Основные подходы к определению понятия<br>4. «компьютерная информация».<br>5. Основные нормативно-правовые акты регулирующие современный информационный оборот. | | | | | | |
| 4. | **Тема 4. Уголовно-правовая природа преступлений в сфере обращения цифровой информации**<br>1. Понятие цифровой информации.<br>2. Понятие преступлений в сфере обращения цифровой информации.<br>3. Феномен безопасной компьютерной атаки. | - | 2 | 1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.<br>2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.<br>3. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.<br>4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве<br>5.Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ.<br>6. Подходы различных государств к уголовно - правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях. | 12 | Устный опрос Проверка практических навыков. | [1] -[6] |
| 5. | **Тема 5. Преступления в сфере компьютерной** | - | 2 | 1. Неправомерный доступ к компьютерной информации (ст. 272 | 12 | Устный опрос Проверка | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации**<br>1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).<br>2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).<br>3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).<br>4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).<br>5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на | | | УК).<br>2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).<br>3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).<br>4. Преступления, совершаемые с использованием глобальных компьютерных сетей. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений.<br>5. Иные преступления, совершаемые с применением компьютерных технологий. | | практических навыков. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). | | | | | | |
| 6. | **Тема 6. Иные виды преступлений в сфере обращения цифровой информации**<br>1. Мошенничество в сфере компьютерной информации.<br>2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.<br>3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.<br>4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.<br>5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. | - | 2 | 1. Причины и условия преступлений в сфере компьютерной информации.<br>2. Особенности личности преступника в сфере компьютерной информации.<br>3. Особенности лиц, совершающих преступления в глобальных компьютерных сетях. | 10 | Устный опрос Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7. | **Тема 7. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации**<br>1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).<br>2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).<br>3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).<br>4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).<br>5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, | - | 2 | 1. Основные направления и система предупреждения преступлений в сфере компьютерной информации.<br>2. Правовое и организационное обеспечение борьбы с преступлениями в сфере компьютерной информации.<br>3. Некоторые проблемы правового регулирования борьбы с преступлениями в сфере компьютерной информации.<br>4. Система правоохранительных органов, осуществляющих борьбу с преступлениями в сфере компьютерной информации. | 10 | Устный опрос<br>Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). | | | | | | |
| 8. | **Тема 8. Иные виды преступлений в сфере обращения цифровой информации**<br>1. Мошенничество в сфере компьютерной информации.<br>2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.<br>3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.<br>4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.<br>5. Приобретение или сбыт цифровой информации, | - | 2 | 1. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ.<br>2. Высокая латентность указанных преступлений и причины. Сложность сбора доказательств и процесса доказывания. Широкий спектр криминалистически значимых признаков преступлений.<br>3. Отсутствие единой программы борьбы с киберпреступлениями. Сложность расследования и раскрытия компьютерных преступлений.<br>4. Отсутствие обобщенной судебной и следственной практики по делам данной категории.<br>5. Нехватка высокопрофессиональных специалистов, представителей правоохранительных органов. | 10 | Устный опрос<br>Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | заведомо добытой преступным путем | | | | | | |
| 9. | **Тема 9. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ**<br>1. Основные направления профилактики преступлений в сфере компьютерной информации.<br>2. Конституционно-правовое регулирование борьбы с преступлениями в сфере компьютерной информации.<br>3. Меры предупреждения преступлений в сфере компьютерной информации.<br>4. Виктимологическая профилактика преступлений в сфере компьютерной информации. | | 2 | 1. Предупреждение преступлений в сфере компьютерной информации.<br>2. Выбор стратегии борьбы с преступлениями в глобальных компьютерных сетях.<br>3. Средства и методы предотвращения | 4 | Устный опрос<br>Проверка практических навыков. | |
| | **Итого** | - | 18 | | 90 | | |

**5.2. Заочная форма обучения**

| № недели | Наименование тем (вопросов), изучаемых по данной дисциплине | Занятия | | Самостоятельная работа обучающихся | | Формы контроля | Литература |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаб. | Содержание | Часы | | |
| 1. | **Тема 1. Уголовно-правовая природа преступлений в сфере обращения цифровой информации** | - | - | 1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. | 10 | Устный опрос<br>Проверка практических | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1. Понятие цифровой информации.<br>2. Понятие преступлений в сфере обращения цифровой информации.<br>3. Феномен безопасной компьютерной атаки. | | | 2. Латентность преступлений в сфере компьютерной информации.<br>3. Оценка общественной опасности и распространенности преступлений в глобальных компьютерных сетях. | | навыков. | |
| 2. | **Тема 2. Научно-технический прогресс и его последствия (побочные эффекты)**<br>4. Научно-техническая революция и социальное развитие.<br>5. Человек – компьютер – преступление.<br>6. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны. | - | 1 | Цифровизация социального пространства как непосредственное влияние на трансформацию права. Внесение дополнений в законодательство, направленные на создание эффективных правовых средств противодействия новым формам криминальной деятельности. Современные цифровые платформы, используемые в уголовном праве, в теории и на практике. Определение понятия «цифровая личность». Преимущества и недостатки создания «цифрового закона». | 10 | Устный опрос<br>Проверка практических навыков. | [1] -[6] |
| 3. | **Тема 3. Основные законы и понятия современного информационного оборота**<br>6. Значение информации в жизни социума.<br>7. Правовое понятие и сущность компьютерной информации.<br>8. Основные подходы к определению понятия<br>9. «компьютерная информация».<br>10. Основные нормативно-правовые акты | - | 1 | Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации | 12 | Устный опрос<br>Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | регулирующие современный информационный оборот. | | | | | | |
| 4. | **Тема 4. Уголовно-правовая природа преступлений в сфере обращения цифровой информации**<br>1. Понятие цифровой информации.<br>2. Понятие преступлений в сфере обращения цифровой информации.<br>3. Феномен безопасной компьютерной атаки. | - | 1 | 1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.<br>2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.<br>3. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.<br>4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве<br>5.Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ.<br>6. Подходы различных государств к уголовно - правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях. | 12 | Устный опрос Проверка практических навыков. | [1] -[6] |
| 5. | **Тема 5. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации**<br>1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).<br>2. Создание, | - | 1 | 1. Неправомерный доступ к компьютерной информации (ст. 272 УК).<br>2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).<br>3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).<br>4. Преступления, совершаемые с использованием глобальных компьютерных сетей. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений.<br>5. Иные преступления, совершаемые с применением компьютерных технологий. | 12 | Устный опрос Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).<br>3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).<br>4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).<br>5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). | | | | | | |
| 6. | **Тема 6. Иные виды преступлений в сфере обращения цифровой информации**<br>1. Мошенничество в | - | 1 | 1. Причины и условия преступлений в сфере компьютерной информации.<br>2. Особенности личности преступника в сфере компьютерной информации. | 10 | Устный опрос Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | сфере компьютерной информации.<br>2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.<br>3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.<br>4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.<br>5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. | | | 3. Особенности лиц, совершающих преступления в глобальных компьютерных сетях. | | | |
| 7. | **Тема 7. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации**<br>1. Неправомерный доступ к компьютерной информации (ст. 272 УК | - | 1 | 1. Основные направления и система предупреждения преступлений в сфере компьютерной информации.<br>2. Правовое и организационное обеспечение борьбы с преступлениями в сфере компьютерной информации.<br>3. Некоторые проблемы правового регулирования борьбы с преступлениями в сфере компьютерной информации.<br>4. Система правоохранительных органов, осуществляющих борьбу с преступлениями в сфере компьютерной информации. | 10 | Устный опрос Проверка практических навыков. | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | РФ).<br>2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).<br>3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).<br>4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).<br>5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). | | | | | | |
| 8. | **Тема 8. Иные виды преступлений в сфере обращения цифровой** | - | 1 | 6. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК | 10 | Устный опрос<br>Проверка практических | [1] -[6] |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **информации**<br>1. Мошенничество в сфере компьютерной информации.<br>2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.<br>3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.<br>4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.<br>5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем | | | РФ.<br>7. Высокая латентность указанных преступлений и причины. Сложность сбора доказательств и процесса доказывания. Широкий спектр криминалистически значимых признаков преступлений.<br>8. Отсутствие единой программы борьбы с киберпреступлениями. Сложность расследования и раскрытия компьютерных преступлений.<br>9. Отсутствие обобщенной судебной и следственной практики по делам данной категории.<br>10. Нехватка высокопрофессиональных специалистов, представителей правоохранительных органов. | | навыков. | |
| 9. | **Тема 9. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ**<br>1. Основные направления профилактики преступлений в сфере компьютерной информации. | | 1 | 1. Предупреждение преступлений в сфере компьютерной информации.<br>2. Выбор стратегии борьбы с преступлениями в глобальных компьютерных сетях.<br>3. Средства и методы предотвращения | 14 | Устный опрос<br>Проверка практических навыков. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2. Конституционно-правовое регулирование борьбы с преступлениями в сфере компьютерной информации.<br>3. Меры предупреждения преступлений в сфере компьютерной информации.<br>4. Виктимологическая профилактика преступлений в сфере компьютерной информации. | | | | | | |
| | **Итого** | - | 8 | | 108 | | |

## 6. Образовательные технологии

Согласно учебному плану в ходе преподавания дисциплины используются традиционные образовательные технологии: лекции, семинарские занятия, самостоятельная работа студентов. Также при проведении занятий и самостоятельной работе студентов могут быть использованы:

- *интерактивные технологии* («мозговой штурм», дебаты, коллоквиумы, презентационный метод, работа в группах и др.);

-*технологии контекстного обучения* – система дидактических форм, методов и средств, направленная на моделирование содержания будущей профессиональной деятельности специалиста (анализ конкретных ситуаций, методы работы с информационными базами данных, моделирование исторических ситуаций и др.);

- *технологии электронного обучения* (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте и с использованием платформ дистанционного обучения (ЭИОС СОГУ).

## 7. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

К видам самостоятельной работы при изучении дисциплины «Профилактика преступлений в сфере компьютерной информации» относятся:

-самостоятельное повторение и изучение теоретического материала;

-выполнение домашних заданий (составление конспекта по изучаемой теме);

-написание докладов, эссе;

-подготовка презентаций;

-самостоятельное изучение исторических источников;

-работа со справочными материалами (терминологическими и иными словарями, энциклопедиями);

-подготовка к промежуточной аттестации (зачету/экзамену).

Содержание, трудоемкость и формы внеаудиторной самостоятельной работы содержатся в разделе 5, табл. 5.1, 5.2.

## 8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины

Рабочая программа предусматривает проведение практических занятий, а также следующие виды

работ: самостоятельную работу студентов по подготовке устных докладов, написанию рефератов, подготовку презентаций и обсуждений по темам дисциплины.

**Виды контроля.**

Рабочая программа предполагает текущий и промежуточный контроль знаний.

**Текущий контроль** - это непрерывно осуществляемый мониторинг уровня усвоения знаний и формирования умений и навыков в течение семестра или учебного года. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию.

Формами текущего контроля могут быть *опросы на практических занятиях, письменные домашние задания по тематике самостоятельной работы, а также подготовка рефератов (докладов),* выполняемые студентами с целью проверки наличия знаний, необходимых для усвоения нового материала и для выяснения степени усвоения изложенного материала.

## Система оценивания текущего контроля успеваемости, соотнесенная с уровнем освоения компетенций

### 8.1. Тематика практических занятий

**Занятие** 1. Уголовно-правовая природа преступлений в сфере обращения цифровой информации

1. Понятие цифровой информации.
2. Понятие преступлений в сфере обращения цифровой информации.
3. Феномен безопасной компьютерной атаки.

**Занятие** 2. Научно-технический прогресс и его последствия (побочные эффекты)

1. Научно-техническая революция и социальное развитие.
2. Человек – компьютер – преступление.

Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны.

**Занятие** 3. Основные законы и понятия современного информационного оборота

1. Значение информации в жизни социума.
2. Правовое понятие и сущность компьютерной информации.
3. Основные подходы к определению понятия
4. «компьютерная информация».
5. Основные нормативно-правовые акты регулирующие современный информационный оборот.

**Занятие** 4. Уголовно-правовая природа преступлений в сфере обращения цифровой информации

1. Понятие цифровой информации.
2. Понятие преступлений в сфере обращения цифровой информации.
3. Феномен безопасной компьютерной атаки

**Занятие** 5. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).

**Занятие 6. Иные виды преступлений в сфере обращения цифровой информации**

1. Мошенничество в сфере компьютерной информации.

2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.

4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

**Занятие 7**. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).

**Занятие 8. Иные виды преступлений в сфере обращения цифровой информации**

1. Мошенничество в сфере компьютерной информации.

2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.

4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем

**Занятие 9. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ**

1. Основные направления профилактики преступлений в сфере компьютерной информации.

2. Конституционно-правовое регулирование борьбы с преступлениями в сфере компьютерной информации.

3. Меры предупреждения преступлений в сфере компьютерной информации.

4. Виктимологическая профилактика преступлений в сфере компьютерной информации.

**8.2.Темы презентаций**

1. Проблемы криминализации деяний в сфере компьютерной информации.

2. Сравнительный анализ российского и зарубежного уголовного законодательства о преступлениях в сфере компьютерной безопасности.

3. Спорные вопросы объективной стороны преступлений в сфере компьютерной информации.

4. Влияние компьютерной техники и информационных технологий на развитие уголовного права России.

5. Вредоносная программа как предмет преступления.

6. Криминологическая характеристика преступлений в сфере компьютерной информации.

7. Анализ воздействия киберпреступности на финансовый и иные сектора экономики.

8. Взаимодействие компьютерной и организованной преступности.

9. Виды и классификация преступлений совершаемых с использованием компьютерных технологий.

10. Перспективные направления совершенствования уголовного законодательства об ответственности за преступления в сфере компьютерной информации.

11. Причины и условия преступлений в сфере компьютерной информации в историческом аспекте.

12. Криминологическая характеристика личности преступника в сфере компьютерной информации.

13. Особенности личности преступника, совершающего преступления в глобальных компьютерных сетях.

14. Борьба с компьютерной преступностью: организационные, правовые и методические аспекты.

15. Перспективы совершенствование системы борьбы с киберпреступностью.

16. Место и роль правовых средств в профилактике компьютерных преступлений.

17. Международное сотрудничество в борьбе с киберпреступностью.

18. Вредоносные программы как средство информационной войны.

19. История вредоносных программ.

20. Информационные отношения как предмет правового регулирования.

21. Понятие и структура информационной безопасности как объекта уголовно - правовой охраны.

22. Информация как предмет преступлений против информационной безопасности.

23. Законодательство РФ в области обеспечения информационной безопасности.

24. Общаяхарактеристика и виды преступлений информационной безопасности по уголовному законодательству зарубежных стран.

25. Проблемы квалификации иных преступлений против информационной безопасности.

26. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).

27. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.

28. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.

29. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка.

30. Перспективные направления совершенствования уголовного законодательства об ответственности за преступления против информационной безопасности.

**Методические рекомендации по созданию мультимедийной презентации**

1.Структура и содержание презентации – это личное творчество автора. Однако полезно использовать шаблоны для оформления и подготовки компьютерной презентации.

2.Слайды не рекомендуется перегружать текстом, лучше разместить короткие тезисы. Наиболее важный материал необходимо выделить.

3.Цифровой материал, плохо воспринимаемый со слайдов, лучше представить в виде графиков и диаграмм.

4.Желательно подготовить к каждому слайду заметки по докладу. Затем распечатать их и использовать при подготовке или на самой презентации.

5.Необходимо соблюдать единый стиль оформления презентации и обратить внимание на стилистическую грамотность.

6.Следует пронумеровать слайды. Это позволит быстро обращаться к конкретному слайду в случае необходимости.

7.Главные выводы по материалу презентации целесообразно поместить на отдельном слайде.

**Критерии оценивания презентаций:**

За выполнение данного вида работы максимальное количество баллов составляет 3 балла, из них:

| **Наименование критерия** | **Критерии оценивания** | | | |
|---|---|---|---|---|
| | **3** | **2** | **1** | **0** |
| **Содержание презентации** | Четко сформулирована цель и раскрыта тема исследования. В краткой форме дана полная информация по теме и дан ответ на проблемный вопрос. Даны ссылки на используемые ресурсы. | Сформулирована цель и тема исследования. Частично изложена информация по теме и дан ответ на проблемный вопрос. Даны ссылки на используемые ресурсы. | Сформулирована цель и тема исследования. Содержание полностью не раскрыто. Информация по теме неточна. Проблема до конца не решена. Не даны ссылки на используемые ресурсы. | Не сформулирована цель и тема. Проблема не решена. |
| **Дизайн презентации** | Соблюдается единый стиль оформления. Презентация красочная и интересная. Используются эффекты анимации, фон, фотографии. В презентации присутствуют авторские находки. | Соблюдается единый стиль оформления. Слайды просты в понимании. Используются некоторые эффекты и фон. | Не соблюдается единый стиль оформления. Слайды просты в понимании. Эффекты и фон не используется. | Не соблюдается стиль оформления. Слайды просты в понимании. |
| **Представление презентации** | Автор хорошо владеет материалом по теме. Использует научную терминологию. Обладает навыками ораторского искусства. Полно и точно цитируется использованная литература | Автор владеет материалом по теме, но не смог заинтересовать аудиторию. Недостаточно цитируется литература. | Автор не показал компетентности в представлении презентации. Использованные факты не вызывают доверия. Недостаточно цитируется литература. | Представлены искаженные данные |

## 8.3. Вопросы для подготовки к промежуточной аттестации

### Вопросы к зачету с оценкой

1. Понятие цифровой информации.
2. Понятие преступлений в сфере обращения цифровой информации.
3. Феномен безопасной компьютерной атаки.
4. Научно-техническая революция и социальное развитие.
5. Человек – компьютер – преступление.
6. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны.
7. Значение информации в жизни социума.
8. Правовое понятие и сущность компьютерной информации.
9. Основные подходы к определению понятия

10. «компьютерная информация».
11. Основные нормативно-правовые акты регулирующие современный информационный оборот.
12. Понятие цифровой информации.
13. Понятие преступлений в сфере обращения цифровой информации.
14. Феномен безопасной компьютерной атаки.
15. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
16. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
17. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).
18. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).
19. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).
20. Мошенничество в сфере компьютерной информации.
21. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
22. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.
23. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.
24. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.
25. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
26. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
27. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).
28. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).
29. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ).
30. Мошенничество в сфере компьютерной информации.
31. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
32. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.
33. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.
34. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем
35. Основные направления профилактики преступлений в сфере компьютерной информации.
36. Конституционно-правовое регулирование борьбы с преступлениями в сфере компьютерной информации.
37. Меры предупреждения преступлений в сфере компьютерной информации.
38. Виктимологическая профилактика преступлений в сфере компьютерной информации.

**8.3.** Зачет проводится в устной форме.

Система оценивания по результатам промежуточного контроля осуществляются в соответствии с Положением СОГУ[1], а также с учетом требований и

[1] Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, магистратуры и

критериев, разработанных преподавателем по данной дисциплине.

Промежуточный контроль - итоговая оценка знаний студента, формируемая по накопительной системе в процессе текущего контроля.

Форма промежуточного контроля – зачет с оценкой.

**Оценивание ответа студента на экзамене по дисциплине**

| ***Уровни*** | ***Характеристика ответа*** | ***оценки*** |
|---|---|---|
| | Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. | отлично |
| | Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. | хорошо |
| | Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. | удовлетворительно |
| | Не получены ответы по базовым вопросам дисциплины. | неудовлетворительно |

## Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

| Уровень сформированности компетенций | | | |
|---|---|---|---|
| **«Минимальный уровень не достигнут»** Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы. | **«Минимальный уровень»** Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка. | «Средний уровень» Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка. | «Высокий уровень» Компетенции сформированы. Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка |
| **Описание критериев оценивания** | | | |
| Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; отсутствие готовности (способности)к дискуссии и низкую степень контактности. | Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; умение без грубых ошибок решать практические задания, которые следует выполнить. | Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в | Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы. |

| | | | |
|---|---|---|---|
| | | раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на вопросы | |
| **Оценка «неудовлетворительно»** | **Оценка «удовлетворительно»** | **Оценка «хорошо»** | **Оценка «отлично»** |

**9. Учебно-методическое и информационное обеспечение дисциплины**

***а) основная литература:***

1. Цифровые технологии в организации судебной и правоохранительной деятельности: учебник для вузов / под редакцией Н. В. Ткачевой. Москва: Издательство Юрайт, 2026. 137 с.

2. Уголовное право. Особенная часть. Семестр I–учебник для вузов / ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. 7-е изд., перераб. и доп. Москва–Издательство Юрайт, 2026. 602 с.

3. Уголовное право. Общая часть: учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. 6-е изд., перераб. и доп. Москва: Издательство Юрайт, 2026. 448 с.

**б) дополнительная литература:**

1. Комментарий к Уголовному кодексу РФ в 4 т. Том 1. Общая часть / В. М. Лебедев [и др.]; ответственный редактор В. М. Лебедев. Москва: Издательство Юрайт, 2026. 316 с.

2. Комментарий к Уголовному кодексу РФ в 4 т. Том 2. Особенная часть. Разделы VII—VIII / В. М. Лебедев [и др.]; ответственный редактор В. М. Лебедев. Москва: Издательство Юрайт, 2026. 371 с.

3. Комментарий к Уголовному кодексу РФ в 4 т. Том 3. Особенная часть. Раздел IX / В. М. Лебедев [и др.]; ответственный редактор В. М. Лебедев. Москва: Издательство Юрайт, 2026. 298 с.

**в) профессиональные базы данных и другие Интернет-ресурсы:**

| | |
|---|---|
| Верховный суд Российской Федерации | http://www.vsrf.ru/ |
| Генеральная прокуратура Российской Федерации | https://epp.genproc.gov.ru/web/gprf |
| Федеральные арбитражные суды | http://arbitr.ru/ |
| Федеральная нотариальная палата | https://notariat.ru/ru-ru/ |
| Федеральная палата адвокатов Российской Федерации | https://fparf.ru/ |
| Сайт Федеральной антимонопольной службы | https://fas.gov.ru |
| Электронная библиотека «Наука права» | https://naukaprava.ru |
| Официальный интернет-портал правовой информации | http://pravo.gov.ru |
| Правовой портал Минюста России «Нормативные правовые акты в Российской Федерации» | http://pravo.minjust.ru |
| Информационно-правовой портал «Гарант» | https://www.garant.ru/ |
| КонсультантПлюс. Надежная правовая поддержка | http://www.consultant.ru/ |
| Юридический сайт об источниках права | https://www.istochnikiprava.ru/ |
| Цивилистика. РФ Интернет-портал о | http://www.civilista.ru/ |

| | |
|---|---|
| науке гражданского права | |
| Библиотека юридической литературы | http://pravo.eup.ru |
| Библиотека юридических редкостей | http://oldlawbook.narod.ru/ |
| Юридический виртуальный клуб Ex - Jure. Библиотека юриста. Новости. Юридическая практика. Интерактив | http://ex-jure.ru/ |
| Профессиональные справочные системы «Кодекс» | https://kodeks.ru/ |

**г) программное обеспечение, ЭБС:**

**- необходимый для обеспечения данной дисциплины комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, а также электронные библиотечные системы, с которыми у СОГУ имеется действующий договор:**

| № п/п | Наименование | № договора(лицензия) | Страна произво-дитель |
|---|---|---|---|
| 1. | Windows 10 Enterprise | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 2. | Windows 10 Pro for Workstations | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 3. | Windows 7 Enterprise | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 4. | Windows 7 Professional | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 5. | Office Standard 2016 | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 6. | Office Standard 2013 | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 7. | Office Standard 2010 | № 4100072800 Microsoft Products (MPSA) от 04.2016 г | США |
| 8. | Корпоративная электронная почта (Яндекс.Почта) | №КИС-1965-2025 от 12.01.2026 | Россия |
| 9. | Программное обеспечение 1С: Предприятие. Бухгалтерский Учет. Типовая конфигурация 8 сетевая версия | № СД/108 от 29.08.2017 «МАКСИМУМ-СОФТ СОФТ» бессрочно | Россия |
| 10. | Система поиска текстовых заимствований «Антиплагиат.ВУЗ» | № SBR003-250010357500001от 05.02.2025 (действителен до 04.02.2026) с ОАО «АнтиПлагиат» | Россия |
| 11. | Программное обеспечение 1С: Предприятие 8.3 Управление торговлей | №КП /108 от 29.08.2017 с ООО «Максимум»(бессрочно) | Россия |
| 12. | Программное | №СД./ №9., 08.06.2025 г. «МАКСИМУМ- | Россия |

| | | | |
|---|---|---|---|
| | обеспечение 1С: Зарплата и кадры государственного учреждения 8 | СОФТ<br>СОФТ» бессрочно | |
| 13. | 1С: Бухгалтерия 8. Базовая версия | №9 от 21.05.2019, «МАКСИМУМ-СОФТ<br>СОФТ» бессрочно | Россия |
| 14. | Планы | №2191-24, от 09.01.2025 г. (тех.поддержка до 26.02.2026 г.) ООО ЛММИС | Россия |
| 15. | ПО Лаборатории ММИС (Деканат, ПК, Ведомости, Тестирование, интернет расширение и др.) | №2435-24 от 04.03.2025<br>ООО ЛММИС | Россия |
| 16. | VSDESK | № 210406/01 от 06.04.2021г. ИП И,А.Сергеевич | Россия |
| 17. | DIRECTUM RX – Система электронного документооборота | ООО Галактика ИТ договор № 120320/Д/А от 14.03.2022 | Россия |
| 18. | MOODLE | Бесплатное | - |
| 19. | ЭБС «Консультант студента» | http://www.studentlibrary.ru<br>Требуется регистрация в библиотеке СОГУ | Россия |
| 20. | РусГард | Бесплатное | Россия |
| 21. | Система веб-конференций (bigbluebutton) | Бесплатное | - |
| 22. | Средства криптографической защиты (КриптоПро CSP, Крипто АРМ) | №120680, от 21.01.2025<br>ООО «Цифровые технологии» | Россия |
| 23. | Средства криптографической защиты (ViPNet) | №0000-000008 от 17.01.2025<br>ООО Экспресс-линк | Россия |
| 24. | Средства криптографической защиты (Континент TLS) | №25/08/22 СЛ от 04.09.2025<br>ООО СКБ-Сервис | Россия |
| 25. | Kaspersky Endpoint Security | № СФ00-001239 от 13.02.2025 ООО Системный Софт | Россия |

Реестр электронных библиотечных систем (ЭБС) и электронных образовательных ресурсов, доступ к которым обеспечен для обучающихся по образовательным программам, реализуемым в 2026-2027 учебном году

| Название базы данных | Платформа и (или) адрес в сети Интернет | Реквизиты | Правообладатель | Количество ключей |
|---|---|---|---|---|
| «Университетская библиотека Online» | https://biblioclub.ru<br>Требуется регистрация. | Договор № 571-12/2025 | ООО «НексМедиа» | Без ограничения количества |

| | | | | |
|---|---|---|---|---|
| Базовая коллекция | | от 12.01.2027 г.<br>С 01.01.2026 г. - 31.12.2026 г. | | пользователей |
| Информационно-аналитическая система SCIENCE INDEX: рефераты и полные тексты научных статей и публикаций, российские научные и научно-технические журналы | eLIBRARY.RU<br>http://elibrary.ru/org<br>Требуется регистрация. | Лицензионный договор<br>№ 310-5051/2025<br>от 31.03. 2025 г.<br>С 14.04.2025 г.-<br>20.04.2026 г. | ООО «Научная электронная библиотека eLibrary.ru» | Доступ по IP адресам вуза без ограничений по количеству пользователей |
| eLIBRARY.RU - интегрированный научный информационный портал в российской зоне сети Интернет, включающий базы данных научных изданий и сервисы для информационного обеспечения науки и высшего образования. | eLIBRARY.RU<br>http://elibrary.ru/org<br>Требуется регистрация. | Ресурс открытого доступа | ООО «Научная электронная библиотека eLibrary.ru» | Доступ осуществляется по IP адресам вуза без ограничений по количеству пользователей |
| «Юрайт»<br>- Учебники по всем специальностям и направлениям подготовки.<br>- ЦУМК по федеральному проекту «Кадры для цифровой экономики» | «Юрайт»<br>https://urait.ru/info/courses? utm_sour...m_campa<br>Требуется регистрация. | Договор № 6237<br>от 05.12.2023 г.<br>С 31.12.2023 -<br>31.12.2026 г. | ООО «Электронное издательство ЮРАЙТ» | Доступ по IP адресам вуза без ограничений по количеству пользователей |
| Универсальная база данных East View<br>- полнотекстовый доступ к научным журналам | https://dlib.eastview.com<br>Логин: Khetagurov.<br>Пароль: Khetagurov. | №210-П от 12.01.2026 г.<br>С 01.01.2026 г.-<br>31.12.2026 г. | ООО «ИВИС» | Без ограничения количества пользователей |
| «SocHum» - электронная библиотека социогуманитарного знания (коллекция учебно-методической литературы и научных журналов социогуманитарной коллекции научно-исследовательских институтов РАН | https://sochum.ru | Ресурс открытого доступа | Государственный академический университет гуманитарных наук (ГАУГН) | Доступ осуществляется по IP адресам вуза без ограничений по количеству пользователей. |
| Polpred.com - открытая электронная библиотечная система и интернет- сервисы «Деловые средства массовой информации».<br>Доступ к статьям 600 газет, журналов информагентств с архивом за 20 лет:<br>- обзор СМИ;<br>- Россия и зарубежье; | https://www.polpred.com/ | Ресурс открытого доступа | | Доступ осуществляется по IP адресам вуза без ограничений по количеству пользователей. |

| | | | | |
|---|---|---|---|---|
| - Федеральные округа РФ.<br>- внешняя экономика, право. | | | | |
| Национальная электронная Библиотека «НЭБ» | https://rusneb.ru/<br>Требуется регистрация. | Договор № 4513-п от 26.12.2023 г. (на 10 лет с последующей автоматической пролонгацией)<br>Без ограничения срока | Российская государственная библиотека | Доступ осуществляется по IP адресам вуза без ограничений по количеству пользователей |

## Электронные образовательные ресурсы

| Наименование ресурса | Содержание ресурса | Ссылка на ресурс в сети Интернет |
|---|---|---|
| Единое окно доступа к образовательным ресурсам | Каталог образовательных интернет-ресурсов и полнотекстовая электронная учебно-методическая библиотека для общего и профессионального образования | https://web.archive.org/web /20191122092928 /http://window.edu.ru/ |
| «КиберЛенинка» | Собрание научных статей, в основном на русском языке, хотя есть и иностранные публикации. | https://cyberleninka.ru/ |
| Всенаука | Естественные, гуманитарные и социальные науки, психология | Всенаука https://vsenauka.ru/ |
| Библиотекарь. Ру | Бесплатная интернет-библиотека. Книги, статьи, документы по русской и мировой истории, искусству, культуре, прикладным наукам, учебники, научные статьи, методические пособия.<br>Электронные книги, учебники, периодика, графика, справочная и техническая литература.<br>На сайте представлено около 10.000 книг доступных для онлайн чтения.<br>- более 50 полнотекстовых справочников и энциклопедий;<br>- Древнерусская литература - летописи, жития святых, воинские повести древней Руси;<br>- сведения иностранных писателей о средневековой России;<br>- большой раздел репринтов книг, газет и журналов 19 века;<br>- биографии и труды русских учёных и писателей;<br>- классическая литература. Мемуары, дневники;<br>- учебники и научные работы по 20 дисциплинам;<br>- более 15.000 картин и художественных изображений. | https://bibliotekar.ru/ |

## 10.Материально-техническоеобеспечениедисциплины(модуля) «Профилактика преступлений в сфере компьютерной информации»

| | |
|---|---|
| Учебная аудитория для проведения занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля № 4и промежуточной аттестации, а также помещения для самостоятельной работы обучающихся № 39: преподавательский стол, стул, столы обучающихся, стулья, кафедра, классная доска, мультимедийный комплекс (проектор, экран), ноутбук, колонки, ПК обучающихся;<br>программное обеспечение:Windows 10 Enterprise№ | Российская Федерация, 362025, Республика Северная Осетия – Алания, г. Владикавказ, улица Бутырина / Бородинская, 27-29/23, учебный корпус 5 |

| | |
|---|---|
| 4100072800 - MicrosoftProducts (MPSA) от 04.2016г; Windows 10 ProforWorkstations- № 4100072800 MicrosoftProducts (MPSA) от 04.2016г; Антивирусное программное обеспечение KasperksyFree, MozillaFirefox, GoogleChrome ( в свободном доступе) ; Гарант - 01.2019-12.2019Консультант+ - №430-2017/614 от11.01.2017 ООО "Фаст-Информ" (бессрочно); | |
| Научная библиотека, в том числе читальный зал с выходом в Интернет: столы стулья, ПК обучающихся, программное обеспечениеEastView (Договор № 310-П от 1-.01.2017 г.), Электронная библиотека «Юрайт» Договор № 1ЭЮ от 27.02.19 Срок действия 01.03.2019г. – 01.03.2020г. Договор №32008816384 Срок действия 01.03.2020 г. -28.02 2021 г. ЭБС "Университетская библиотека Online (Договор №171-12,2019 от 10.02.2020 г.) Электронная библиотека диссертаций и авторефератов РГБ (ЭБД РГБ) (Договор №095/04/0130 от 01.07.2019); Научная электронная библиотека eLibrary.ru Лицензионное соглашение № 5051 от 02.09.2009 г. Бессрочное | Российская Федерация, 362025, Республика Северная Осетия – Алания, г. Владикавказ, улица Бутырина / Бородинская, 27-29/23, учебный корпус 5 |