

Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по учебной работе  
д.юр.н., доц. Васильева Н.В.



21.06.2024г.

**Рабочая программа дисциплины**  
Б1.Э.1. Кибервиктимология

Направление подготовки: 40.04.01 Юриспруденция  
Направленность (профиль): Криминалистика, судебная экспертиза и  
оперативно-розыскная деятельность  
Квалификация выпускника: магистр  
Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	2	2
Семестр	21	22
Лекции (час)	14	24
Практические (сем, лаб.) занятия (час)	14	0
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	116	120
Курсовая работа (час)		
Всего часов	144	144
Зачет (семестр)		
Экзамен (семестр)	21	22

Иркутск 2024

Программа составлена в соответствии с ФГОС ВО по направлению 40.04.01  
Юриспруденция.

Авторы Д.В. Жмуров, нет

Рабочая программа обсуждена и утверждена на заседании кафедры  
уголовного права и криминологии

Заведующий кафедрой Т.М. Судакова

## 1. Цели изучения дисциплины

Целью освоения дисциплины кибервиктимология является получение студентами знаний о жертвах преступлений в виртуальном пространстве, а также о средствах, формах и масштабах виктимизации в сети Интернет.

Это актуальная проблема связана со всё возрастающим числом потерпевших в виртуальной среде: по оценкам экспертов мировая экономика в 2022 году может потерять от деятельности кибермошенников до восьми триллионов долларов, а в 2030-м - более 90 [Жданов, 2020]; к 2023 году около 30% нарушений уголовного кодекса может перейти в Сеть [Сидоренко, 2020]; а 64% россиян уже становились жертвами киберпреступников [по данным Mail Group и Neilsen]. В сложившейся ситуации представленный учебный курс позволит студентам ориентироваться в актуальной повестке, получить сведения о распространенности киберпреступности, типах виктимизирующих воздействий, а также необходимых средствах виктимологической профилактики.

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

### Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции по ФГОС ВО	Компетенция
ПК-5	Способен применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации

### Структура компетенции

Компетенция	Формируемые ЗУНы
ПК-5 Способен применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации	З. Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У. Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации

## 3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Элективная дисциплина.

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

Общая трудоемкость дисциплины составляет 4 зач. ед., 144 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		

Лекции	14	24
Практические (сем, лаб.) занятия	14	0
Самостоятельная работа, включая подготовку к экзаменам и зачетам	116	120
Всего часов	144	144

**5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**5.1. Содержание разделов дисциплины**

**Заочная форма обучения**

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Теоретические и методологические основы кибервиктимологии	22	4		12		Задание № 1.. Решение задач. Тестирование
2	Кибервиктимность, как новая категория VUCA-мира	22	4		12		Задание № 2
3	Кибервиктимизация. Интегративный подход и научно-исследовательская матрица	22	2		12		Задание № 3
4	Кибержертва: решение проблемы терминологической неопределенности	22	2		12		Задание № 4
5	Факторы кибервиктимизации	22	2		12		Задание № 5
6	Виктимологическая характеристика преступлений, связанных с повреждением сетевой инфраструктуры	22	2		15		
7	Виктимологическая характеристика интернет-мошенничества	22	2		15		Задание № 7
8	Виктимологическая характеристика феномена фейка	22	4		15		Задание № 8
9	Виктимологическая характеристика кибербуллинга и киберсталкинга	22	2		15		Задание № 6. Задание № 9

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
	ИТОГО		24		120		

#### Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Теоретические и методологические основы кибервиктимологии	21	2	4	12		Задание № 1.. Решение задач. Тестирование
2	Кибервиктимность, как новая категория VUCA-мира	21			12		Задание № 2
3	Кибервиктимизация. Интегративный подход и научно-исследовательская матрица	21	2		12		Задание № 3
4	Кибержертва: решение проблемы терминологической неопределенности	21	2		12		Задание № 4
5	Факторы кибервиктимизации	21	2		12		Задание № 5
6	Виктимологическая характеристика преступлений, связанных с повреждением сетевой инфраструктуры	21	2	2	15		
7	Виктимологическая характеристика интернет-мошенничества	21	2	2	11		Задание № 7
8	Виктимологическая характеристика феномена фейка	21		4	15		Задание № 8
9	Виктимологическая характеристика кибербуллинга и киберсталкинга	21	2	2	15		Задание № 6. Задание № 9
	ИТОГО		14	14	116		

#### 5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Лекция № 1	Понятие кибервиктимологии, ее предмет. Ключевые методы исследования и эволюционные перспективы.

№ п/п	Наименование разделов и тем	Содержание
2	Лекция № 2	Понятие кибервиктимности. Отход от классической виктимологии: тезис «комменсализм на смену хищничества». Новые парадигмы причинения криминального вреда в интернете. Размывание понятия субъект индивидуальной виктимизации: сложные самоорганизующиеся системы и IoT, как жертвы преступных посягательств.
3	Лекция № 3	Понятие кибервиктимизации, ее гипотетическая модель (модель-ПОРПЭ): профилирование, обусловленность, распространенность, прогнозируемость, эпидемичность. Номенклатура ключевых актов кибервиктимизации: пятнадцать глобальных категорий и около ста акцентных форм. Среди глобальных: угрозы; преследование; незаконный интерес; остракизм; обвинение или навешивание ярлыков; персональная дискредитация; подмена личности; разглашение; внушение; изъятие; повреждение сетевой инфраструктуры; организационная компрометация; пользование чужими ресурсами; пользование чужими предпочтениями; создание необоснованных ожиданий.
4	Лекция № 4	Кибержертва и субъект кибервиктимизации: ключевые дефиниции. Сущностные характеристики кибержертв, отличающие от их традиционных жертв преступлений; разграничение со смежными понятиями, например, лицами, пострадавшими на фоне персональной интернет-активности, потерпевшими от преступлений в сфере компьютерной информации. Классификация кибержертв, включающая цифровых, комбинированных и неvirtуальных потерпевших.
5	Лекция № 5	Обстоятельства, вызывающие реализацию виктимного потенциала в сети. Их виды и классификация: а) поведенческие триггеры, проявляющиеся в виктимном образе действий; б) психологические триггеры, выражающиеся в психической деятельности человека и ее виктимогенных проявлениях; в) социальные триггеры, связанные с межличностным и групповым взаимодействием; г) технические триггеры, как комплекс условий, относящийся к инфраструктуре, формирующей отраслевые виктимогенные риски. Сюда входят: стремительная цифровизация и сменяющие друг друга технологические уклады, несовершенство и уязвимости компьютерных систем, непредвиденные или заложенные программные ошибки, риски, связанные с дистанционным обслуживанием и проч.
6	Лекция № 6	Характеристика жертв технических атак на серверы и объекты интернет-инфраструктуры. Классификация форм виктимизации.
7	Лекция № 7	Характеристика форм интернет-мошенничества и сопутствующие им скрипты виктимизации.
8	Лекция № 8	Виктимизация личности от потребления ею ложной, некачественной или искаженной медиа-информации. Фейк, как генерализованное понятие, охватывающее опасные, с т.з. информационной гигиены, медиа-данные. Дефиниция и классификация фейков.

№ п/п	Наименование разделов и тем	Содержание
9	Лекция № 9	Формы проявления и виды кибербуллинга (киберсталкинга). Физические и психологические последствия этих форм дискриминации.

### 5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Практическое занятие № 1. Проводится в форме беседы. Понятие кибервиктимологии и ее предмет. Цели и задачи науки. Современное состояние исследований.
2	Практическое занятие № 2. Проводится в форме беседы. Кибервиктимность, как понятие выходящее за пределы классической виктимологии. Изменение парадигмы причинения преступного вреда в виртуальном пространстве. Субъекты кибервиктимизации и жертвы киберпреступлений.
3	Практическое занятие № 3. Проводится в форме беседы. Кибервиктимизация. Подходы к оценке феномена. Формы проявления. Оценка распространенности.
4	Практическое занятие № 4. Проводится в форме беседы. Кибержертва. Ее типические характеристики (виктимная амбивалентность, деперсонифицированность, экстерриториальность, особые персональные качества, смешанный технико-личностный характер виктимности). Виды интернет потерпевших: а) жертвы имущественной; б) экономической компрометации; в) жертвы вовлечения; г) агрессии; д) деструктивных действий (разрушения); е) нарушения информационных прав; ж) жертвы сервиса.
5	Практическое занятие № 5. Проводится в форме беседы. Характеристика факторов кибервиктимизации различных уровней и содержания (поведенческих, психологических, социальных, технических).
6	Практическое занятие № 6. Проводится в форме беседы. Субъекты виктимизации связанной с повреждением сетевой инфраструктуры. Формы виктимизирующих действий: <ul style="list-style-type: none"> <li>• _Вмешательство в доступ или использование чужого компьютера (DDoS-атаки, атаки парольные, подслушивающие, приводные, с использованием искусственного интеллекта и проч.)</li> <li>• _Ботнеты</li> <li>• _Эксллойты</li> <li>• _SQL инъекции</li> <li>• _Кража паролей FTP</li> <li>• _Межсайтовые сценарии</li> <li>• _Логические бомбы</li> <li>• _Угон сайтов</li> <li>• _Дидлинг</li> <li>• _Вредоносные программы</li> <li>• _Использование шифрования в помощь преступлению;</li> <li>• _Фальсификация исходной информации электронной почты</li> <li>• _Кража информационных услуг провайдера</li> <li>• _Бэждор</li> <li>• _Руткит</li> </ul>

№ раздела и темы	Содержание и формы проведения
	<ul style="list-style-type: none"> <li>• _Инсайдерские угрозы</li> <li>• _Физинг/Спуфинг</li> </ul>
7	<p>Практическое занятие № 7. Проводится в форме беседы. Характеристика виктимизации от интернет-мошенничества. Подробный анализ следующих форм виктимизации:</p> <ul style="list-style-type: none"> <li>• _Ложное трудоустройство</li> <li>• _Работа на дому</li> <li>• _Трудоустройство без оплаты</li> <li>• _Кредитные аферы</li> <li>• _Денежные переводы</li> <li>• _Нарушение приватности финансовых операций</li> <li>• _Инвестиции в бизнес</li> <li>• _Инвестиции в финансовые инструменты</li> <li>• _Обмен валют</li> <li>• _Страхование</li> <li>• _Лотереи и тотализаторы</li> <li>• _Казино</li> <li>• _Букмекерские услуги</li> <li>• _Продажа медицинского оборудования и препаратов</li> <li>• _Консультационные услуги медицинских работников</li> <li>• _Консультационные услуги колдунов, магов, целителей</li> <li>• _Помощь в оформлении справок, рецептов, записи на прием, получении медицинских документов</li> <li>• _Кража личных данных</li> <li>• _СМС-мошенничества</li> <li>• _Фейковые курсы и интернсивы</li> <li>• _Доступ к ресурсам</li> <li>• _Доступ к программам</li> <li>• _Продажа несуществующих товаров и оказание мнимых услуг</li> <li>• _Покупка реальных товаров и услуг</li> <li>• _Мошенничество с программами лояльности</li> <li>• _Мошенничество в области социальной помощи</li> <li>• _Лжеответственность</li> <li>• _Официальная помощь в реализации государственных услуг</li> <li>• _Неофициальная помощь в реализации государственных услуг</li> <li>• _Мошенничества на доверии</li> <li>• _Лжеблаготворительность</li> </ul>
8	<p>Практическое занятие № 8. Проводится в форме беседы. Виды фейков. Криминальные последствия распространения фейковой информации. Причинение смерти по неосторожности, иные летальные случаи, вызванные слухами и фейками. Классификация фейк-мейкеров. Дипфейки и порнографические фейки. Жертвы фейковой дезинформации.</p>
9	<p>Практическое занятие № 9. Проводится в форме беседы. Виктимологическая характеристика кибербуллинга и киберсталкинга (интернет-преследование в широком смысле слова, пранкинг, бомбардировка зумом (зумбомбинг); тематическое преследование (гендерное, сексистское, политическое, религиозное); домогательства, в т.ч. продолжительные; нежелательные комментарии; создание целевого контента для издевательств над жертвой; организация личных встреч для целей персональной дискриминации)</p>

**6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)**

**6.1. Текущий контроль**

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.n, У.1...У.n, Н.1...Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	1. Теоретические и методологические основы кибервиктимологии	ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н.Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 1.	Правильность выполнения задания (4)
2		ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н.Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Решение задач	Правильное решение задач по теме (20)
3		ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства	Тестирование	Правильное решение тестовых заданий (40)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			собрания, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками сбора, исследования, оценки и использования криминалистически значимой информации		
4	2. Кибервиктимность, как новая категория VUCA-мира	ПК-5	З. Знает методы и средства сбора, исследования, оценки и использования криминалистически значимой информации У. Умеет применять методы и средства сбора, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками сбора, исследования, оценки и использования криминалистически значимой информации	Задание № 2	Правильность выполнения задания (4)
5	3. Кибервиктимизация. Интегративный подход и научно-исследовательская матрица	ПК-5	З. Знает методы и средства сбора, исследования, оценки и использования криминалистически значимой информации У. Умеет применять методы и средства сбора, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками сбора, исследования, оценки и использования криминалистически значимой информации	Задание № 3	Правильность выполнения задания (4)
6	4. Кибержертва: решение проблемы	ПК-5	З. Знает методы и средства сбора, исследования, оценки	Задание № 4	Правильность выполнения задания (4)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п))	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
	терминологической неопределенности		и использования криминалистически значимой информации У. Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации		
7	5. Факторы кибервиктимизации	ПК-5	З. Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У. Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 5	Правильность выполнения задания (4)
8	7. Виктимологическая характеристика интернет-мошенничества	ПК-5	З. Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У. Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н. Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 7	Правильность выполнения задания (5)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			криминалистически значимой информации		
9	8. Виктимологическая характеристика феномена фейка	ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н.Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 8	Правильность выполнения задания (5)
10	9. Виктимологическая характеристика кибербуллинга и киберсталкинга	ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации Н.Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 6	Правильность выполнения задания (5)
11		ПК-5	З.Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации У.Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации	Задание № 9	Правильность выполнения задания (5)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1...З.п, У.1...У.п, Н.1...Н.п))	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			значимой информации Н. Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации		
				<b>Итого</b>	<b>100</b>

## 6.2. Промежуточный контроль (зачет, экзамен)

### Рабочим учебным планом предусмотрен Экзамен в семестре 21.

#### ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (40 баллов), вид вопроса: Тест/проверка знаний. Критерий: Глубоко и всесторонне аргументирует свои взгляды по дискуссионным теоретическим вопросам кибервиктимологии; показывает отличные навыки по анализу динамики, состояния, структуры интернет-жертв, выявлению и определению причинного комплекса виктимизации в сети Интернет; разрабатывает программы виктимологического контроля над преступностью. Базовый. Демонстрирует знание теоретических положений курса «Кибервиктимология», знает существующие взгляды по дискуссионным теоретическим вопросам кибервиктимологии; владеет навыками оценки виктимологической ситуации; анализа динамики состояния, структуру преступности, ее причинного комплекса виртуальной виктимизации. Минимальный. Демонстрирует знание некоторых теоретических положений курса «Кибервиктимология», знает некоторые существующие взгляды по дискуссионным теоретическим вопросам кибервиктимологии; имеет представление о ее основных категориях и направлениях исследования..

**Компетенция: ПК-5 Способен применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации**

Знание: Знает методы и средства собирания, исследования, оценки и использования криминалистически значимой информации

1. Кибервиктимность и кибервиктимизация, как новая категория VUCA-мира
2. Теоретические и методологические основы кибервиктимологии

#### ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

2-й вопрос билета (40 баллов), вид вопроса: Задание на умение. Критерий: Точно и всесторонне аргументирует свои взгляды по дискуссионным теоретическим вопросам кибервиктимологии; успешно справляется с поставленными заданиями в сфере использования цифровых образовательных технологий и проч..

**Компетенция: ПК-5 Способен применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации**

Умение: Умеет применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации

Задача № 1. Разработка ментальной карты по теме занятия на ресурсе <https://www.mindmeister.com/ru>

Задача № 2. Самостоятельное проведение интернет-анкетирования при помощи специализированных социологических порталов (Анкетолог, SurveyMonkey)

#### ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

3-й вопрос билета (20 баллов), вид вопроса: Задание на навыки. Критерий: Со всеми необходимыми объяснениями решает задачи; показывает отличные навыки по анализу динамики, состояния, структуры виктимизации, без особых трудностей определяет тип кибержертвы, форму виртуальной виктимизации и проч..

**Компетенция: ПК-5 Способен применять методы и средства собирания, исследования, оценки и использования криминалистически значимой информации**

Навык: Владеет навыками собирания, исследования, оценки и использования криминалистически значимой информации

Задание № 1. Так , гр. К., преследуя возникший корыстный умысел, при помощи принадлежащего ему мобильного телефона, создал от...

#### ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «БГУ»)</b>	Направление - 40.04.01 Юриспруденция Профиль - Криминалистика, судебная экспертиза и оперативно-розыскная деятельность Кафедра уголовного права и криминологии Дисциплина - Кибервиктимология
---	---

#### ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (40 баллов).
2. Самостоятельное проведение интернет-анкетирования при помощи специализированных социологических порталов (Анкетолог, SurveyMonkey) (40 баллов).
3. Так , гр. К., преследуя возникший корыстный умысел, при помощи принадлежащего ему мобильного телефона, создал от... (20 баллов).

Составитель \_\_\_\_\_ Д.В. Жмуров

Заведующий кафедрой \_\_\_\_\_ Т.М. Судакова

**7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)**

**а) основная литература:**

1. Ившин В. Г. Владимир Георгиевич, Идрисова С. Ф. Светлана Феликсовна, Татьяна Л. Г. Лариса Геннадьевна Виктимология. учеб. пособие [для вузов]/ В. Г. Ившин, С. Ф. Идрисова, Л. Г. Татьяна.- М.: Волтерс Клувер, 2011.-253 с.
2. Варчук Т. В., Вишневецкий К. В. Виктимология. 2-е изд., перераб. и доп./ Т.В. Варчук.- Москва: Юнити-Дана, 2015.-191 с.
3. Федоров А. В., Чернов А. В. Виктимология как частная криминологическая теория/ А. В. Федоров, А. В. Чернов.- Иркутск: ВСИ МВД России, 2004.-143 с.
4. Жмуров Д.В. Курс лекции по криминологии в схемах и таблицах.- 180 с.
5. [Криминология : учебно-методическое пособие / Г.Т. Журавлев, Е.В. Ковалевская. — Москва : Евразийский открытый институт, 2009. — 184 с. — ISBN 978-5-374-00179-2. Режим доступа: <https://www.book.ru/book/905531>](#)

**б) дополнительная литература:**

1. Мощицкая Е. Ю. Елена Юрьевна, Репецкая А. Л. Виктимологическая характеристика сексуального насилия несовершеннолетних (по материалам Иркутской области). 12.00.08. дис. ... канд. юрид. наук/ Мощицкая Елена Юрьевна.- Иркутск, 2004.-189 л.
2. Бобраков И. Виктимологические аспекты посягательств, совершенных в отношении участников уголовного судопроизводства/ И. А. Бобраков// С. 56-58, N 3., 2005, ч.з 2-202
3. Джаянбаев К. Виктимологические аспекты предупреждения тяжких преступлений против личности/ К. И. Джаянбаев// Государство и право
4. Минская В. С., Чечель Г. И. Виктимологические факторы и механизм преступного поведения/ В. С. Минская, Г. И. Чечель.- Иркутск: Изд-во Иркут. ун-та, 1988.-151 с.
5. Гарипов И. М. Виктимологическое направление воздействия на криминальное коррупционное поведение: понятие, содержание и основные виды/ И. М. Гарипов// Следователь
6. Жмуров Д.В. Криминология. Русско-английский актуальный словарь.- Москва, 2015.- 140 с.
7. [Бобраков И.А. Криминологическое изучение и предупреждение насильственных преступлений против правосудия, совершаемых в отношении свидетелей и потерпевших \[Электронный ресурс\] : монография / И.А. Бобраков, О.П. Волошина. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2013. — 142 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/13858.html>](#)
8. [Косарев Виктор Николаевич К вопросу о формировании личности преступника // Бизнес в законе. 2009. №1. URL: <http://cyberleninka.ru/article/n/k-voprosu-o-formirovanii-lichnosti-prestupnika>](#)
9. [Райков А.Е., Равнянский А.К. Экономико-криминологическая характеристика государственной политики в сфере борьбы с наркопреступностью в России / А.Е. Райков, А.К. Равнянский \[Электронный ресурс\] // Научные исследования и разработки молодых ученых. 2015. 33. С. 206-211. – Режим доступа: <http://elibrary.ru/item.asp?id=23028888> \(01.11.2016\)](#)

**8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы**

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

- Сайт Байкальского государственного университета, адрес доступа: <http://bgu.ru/>, доступ круглосуточный неограниченный из любой точки Интернет
- Библиотека Псифактор (библиотека научной литературы по массмедиа, СМИ, пропаганде, философии, психологии массовой коммуникации, журналистики), адрес доступа: <http://psyfactor.org/lybr.htm>. доступ неограниченный
- Библиотека Славы Янко, адрес доступа: <http://yanko.lib.ru/gum.html>. доступ неограниченный

- Глобалтека. Глобальная библиотека научных ресурсов, адрес доступа: <http://globalteka.ru>. доступ неограниченный
- КиберЛенинка, адрес доступа: <http://cyberleninka.ru>. доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области уголовного права и криминологии.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

- текущие консультации;
- коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);
- прием и разбор домашних заданий (в часы практических занятий);
- прием и защита лабораторных работ (во время проведения занятий);
- выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
- написание рефератов, докладов;
- подготовка к семинарам и лабораторным работам;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения**

В учебном процессе используется следующее программное обеспечение:

- 7-Zip,
- MS Office,

- WinDjView,
- Adobe Flash player,

#### **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):**

В учебном процессе используется следующее оборудование:

- Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза,
- Учебные аудитории для проведения: занятий лекционного типа, занятий семинарского типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения,
- Наборы демонстрационного оборудования и учебно-наглядных пособий