DOI 10.17150/2411-6262.2021.12(3).25 http://brj-bguep.ru

УДК 343.988

Д.В. Жмуров
Байкальский государственный университет,
г. Иркутск, Российская Федерация

КИБЕРВИКТИМОЛОГИЯ, КАК НОВАЯ УЧЕБНАЯ ДИСЦИПЛИНА: МЕТОДИЧЕСКАЯ РАЗРАБОТКА

АННОТАЦИЯ. Представлена авторская учебно-методическая разработка курса «Кибервиктимология», призванная сформировать у студентов научно-исследовательские компетенции в рамках магистерской программы «Уголовное право и криминология» (направление подготовки «Юриспруденция»). Кроме названной, ключевыми целями настоящего учебного курса являются: а) информирование подопечных о наиболее актуальных процессах, происходящих в современной преступности, об специфических свойствах и изменениях статуса жертв киберпреступлений и лиц, пострадавших в кибернетической среде; б) развитие профессиональных компетенций, связанных с эффективностью будущей работы в правоохранительной сфере; в) развитие навыков цифровой гигиены. В рамках настоящей учебно-методической разработки охарактеризована актуальность предлагаемого учебного курса, описаны его цели и задачи, предложена структура лекционных и семинарских занятий, детально раскрыты цифровые дидактические технологии, применение которых предполагается в ходе обучения по настоящему предмету. В завершении раскрыты некоторые формы итогового контроля (тестовые вопросы, вопросы к зачету), которые бы могли использоваться для проверки знаний.

КЛЮЧЕВЫЕ СЛОВА. Кибервиктимология, научные исследования, учебно-методический комплекс, жертвы в цифровом пространстве, кибервиктимность, кибервиктимизация.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 9 мая 2021 г.; дата принятия к печати 19 июля 2021 г.; дата онлайн-размещения 31 августа 2021 г.

D.V. Zhmurov
Baikal State University,
Irkutsk, Russian Federation

CYBERVICTIMOLOGY AS A NEW COURSE UNIT: METHODOLOGICAL GUIDANCE

ABSTRACT. The author's own teaching guide of the course "Cybervictimology" is presented. It is aimed at developing students' scientific and research competencies within in the Master's degree program "Criminal Law and Criminology" (major field of study is "Law"). Apart from that, the key objectives of the academic course are as follows: a) to inform students about the most relevant processes in the modern criminality, and specificities and changes in the status of victims afflicted by cybercrimes; b) to develop professional competencies related to efficiency of the future occupation in law enforcement; c) to develop skills of digital hygiene. Relevance of the proposed training course, its goals and tasks are described. The structure of lectures and seminars is outlined. Digital didactic technologies to be used in the course are detailed. To complete the course, a number of final testing forms (test questions, credit questions) ensuring quality of the acquired knowledge are introduced.

KEYWORDS. Cybervictimology, scientific researches, academic and methodological complex, victims in digital environment, cybervictimity, cybervictimization.

ARTICLE INFO. Received May 9, 2021; accepted July 19, 2021; available online August 31, 2021.

Актуальность учебно-методического комплекса

Рост киберпреступности, фиксируемый с 2013 по 2020 г. достиг 20-тикратных значений [1]. Это не может быть оставлено без внимания со стороны общества и государства. Цифровая трансформация неизбежно повлекла эволюционные изменения криминальной сферы [2]. Набирающая силу киберпреступность, расширение ее масштабов и диверсификация, диктуют необходимость контроля последней. В противном случае возникает вопрос о дееспособности государства в части выполнения им правоохранительных обязательств. Одним из способов достижения упомянутого контроля является профилактическая работа с потенциальными жертвами и их девиктимизация, т.е. уменьшение опасности провоцирующего поведения в Интернете. Эффективность подобной работы зависит от качества подготовки специалистов новых формаций — киберкриминалистов, кибервиктимологов и проч. Данная задача представляется весьма актуальной и нуждается в практической поддержке: не только артикулировании и декларировании, но и создании реальных образовательных инструментов.

В рамках этой идеи целесообразно создание нового учебного предмета, именуемого кибервиктимология. Его можно определить, как междисциплинарную область, исследующую виктимизацию пользователей в виртуальном пространстве объединенных компьютерных сетей. Это направление исследований имеет перспективы развития и связано со все возрастающими темпами виктимизации людей в цифровой среде. Тем более, что потребность в модернизации концептуальных и теоретических основ российской криминологии назрела уже давно [3].

Появление данного направления исследований и учебного предмета вполне закономерно. По мнению педагогов, оно отражает прогресс науки, техники и изменения в общественной жизни [4]. Это происходит на фоне возрастания объема научной информации, влечет необходимость ее обобщения и, как следствие, создание новых учебных курсов [5].

Цель учебного курса

Выражается в триединстве дидактических, развивающих и воспитательных целей. Это закрепление знаний, развитие способностей и воспитание профессионально-значимых качеств по выбранному предмету. Данная цель конкретизируется в обучении специалистов, обладающих исследовательскими и аналитическими компетенциями в области кибервиктимизации, способных адекватно реагировать на цифровые угрозы, противопоставлять им стратегии совладания, а также самостоятельно проводить научные исследования в указанной сфере.

Задачи учебного курса

Из поставленной цели вытекает ряд задач, отраженных в триаде «знания-умения-навыки». Рассмотрим каждый из этих элементов отдельно:

Знания представлены в:

– концептуальных и понятийных основах кибервиктимологии;

– сведениях о причинах и условиях, виктимологических особенностях совершения отдельных киберпреступлений;

– информации о методах и средствах поиска, обработки научных и правовых данных.

Умения отражены во владении системой современных информационных технологий, применяемых для целей исследовательской деятельности:

– при разработке ментальных и интеллект-карт: https://www.mindmeister.com/ru;

– проведении социологических исследований: https://anketolog.ru/, https://www.google.ru/forms/, https://ru.surveymonkey.com;

– символьном изображении информации, например, https://yequalx.com/ru/chart;

– при работе с библиографическими данными: https://www.mendeley.com, https://www.elibrary.ru/;

– осуществлении статистической аналитики: https://www.statista.com/;

– для разработки тестовых материалов: https://www.survio.com/, https://master-test.net/, https://www.testograf.ru/;

– организации и проведению научных мероприятий онлайн: https://event.4science.ru/

Навыки, как способности к автоматизированной деятельности, включают:

– способность сбора, систематизации и обработки информации для целей виктимологической профилактики с применением современных информационных технологий;

– квалификацию в организации научно-практических исследований и мероприятий с применением современных информационных технологий.

План курса. Основная часть курса

Курс «Кибервиктимология» состоит из 9 основных тем, в которых раскрываются основные аспекты формирования и функционирования жертв криминальных действий в сети интернет. Данный курс предназначен для будущих сотрудников правоохранительных органов, криминальных юристов, криминологов.

Темы курса были подобраны таким образом, чтобы обеспечить студентов:

– современными знаниями о жертвах в цифровом обществе;

– необходимыми компетенциями, связанными с эффективной будущей работой в правоохранительной системе, а также в сфере цифровой гигиены;

– исследовательскими компетенциями на базе современных цифровых технологий.

Содержание лекционных и семинарских занятий целесообразно представить специальной таблице ниже.

Лекционные и семинарские занятия курса «Кибервиктимология»

Наименование разделов и тем	Содержание лекционных занятий	Содержание семинарских занятий
Теоретические и методологические основы кибервиктимологии	Понятие кибервиктимологии, ее предмет. Ключевые методы исследования и эволюционные перспективы.	Понятие *кибервиктимологии* и ее предмет. Цели и задачи науки. Современное состояние исследований.
Кибервиктимность, как новая категория VUCA-мира	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.	*Кибервиктимность*, как понятие выходящее за пределы классической виктимологии. Изменение парадигмы причинения преступного вреда в виртуальном пространстве. Субъекты кибервиктимизации и жертвы киберпреступлений.

Продолжение табл.

Наименование разделов и тем	Содержание лекционных занятий	Содержание семинарских занятий
Кибервиктимизация. Интегративный подход и научно-исследовательская матрица	Понятие кибервиктимизации, ее гипотетическая модель (модель-ПОР-ПЭ): 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 преференциями; создание необоснованных ожиданий.	*Кибервиктимизация*. Подходы к оценке феномена. Формы проявления. Оценка распространенности.
Кибержертва: решение проблемы терминологической не-определенности	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 невиртуальных потерпевших.	*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.
Факторы кибервиктимизации	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.	*Характеристика факторов кибервиктимизации* различных уровней и содержания (поведенческих, психологических, социальных, технических).

Продолжение табл.

Наименование разделов и тем	Содержание лекционных занятий	Содержание семинарских занятий
Виктимологическая характеристика преступлений, связанных с повреждением сетевой инфраструктуры	Характеристика жертв технических атак на серверы и объекты интернет-инфраструктуры. Классификация форм виктимизации.	*Субъекты виктимизации связанной с повреждением сетевой инфраструктуры*. Формы виктимизирующих действий: – Вмешательство в доступ или использование чужого компьютера (DDoS-атаки, атаки парольные, подслушивающие, приводные, с использованием искусственного интеллекта и проч.) – Ботнеты – Экслойты – SQL инъекции – Кража паролей FTP – Межсайтовые сценарии – Логические бомбы – Угон сайтов – Дидлинг – Вредоносные программы – Использование шифрования в помощь преступлению; – Фальсификация исходной информации электронной почты – Кража информационных услуг провайдера – Бэкдор – Руткит – Инсайдерские угрозы – Физинг/Спуфинг
Виктимологическая характеристика феномена фейка	Виктимизация личности от потребления ею ложной, некачественной или искаженной медиа-информации. Фейк, как генерализованное понятие, охватывающее опасные, с точки зрения информационной гигиены, медиа-данные. Дефиниция и классификация фейков.	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.
Виктимологическая характеристика кибербуллинга и киберсталкинга	Формы проявления и виды кибербуллинга (киберсталкинга). Физические и психологические последствия этих форм дискриминации.	Виктимологическая характеристика кибербуллинга и киберсталкинга (интернет-преследование в широком смысле слова, пранкинг, бомбардировка зумом (зумбомбинг); тематическое преследование (гендерное, сексистское, политическое, религиозное); домогательства, в том числе продолжительные; нежелательные комментарии; создание целевого контента для издевательств над жертвой; организация личных встреч для целей персональной дискриминации)

Окончание табл.

Наименование разделов и тем	Содержание лекционных занятий	Содержание семинарских занятий
Виктимологическая характеристика интернет-мошенничества	Характеристика форм интернет-мошенничества и сопутствующие им скрипты виктимизации.	*Характеристика виктимизации от интернет-мошенничества*. Подробный анализ следующих форм виктимизации: – Ложное трудоустройство – Работа на дому – Трудоустройство без оплаты – Кредитные аферы – Денежные переводы – Нарушение приватности финансовых операций – Инвестиции в бизнес – Инвестиции в финансовые инструменты – Обмен валют – Страхование – Лотереи и тотализаторы – Казино – Букмекерские услуги – Продажа медицинского оборудования и препаратов – Консультационные услуги медицинских работников – Консультационные услуги колдунов, магов, целителей – Помощь в оформлении справок, рецептов, записи на прием, получении медицинских документов – Кража личных данных – СМС-мошенничества – Фейковые курсы и интернсивы – Доступ к ресурсам – Доступ к программам – Продажа несуществующих товаров и оказание мнимых услуг – Покупка реальных товаров и услуг – Мошенничество с программами лояльности – Мошенничество в области социальной помощи – Лжеответственность – Официальная помощь в реализации государственных услуг – Неофициальная помощь в реализации государственных услуг – Мошенничества на доверии – Лжеблаготворительность

Цифровые технологии в обучении

Использование указанных технологий подкрепляется совокупностью исследовательских стратегий, основанных на использовании современных цифровых методов исследования и научной коммуникации (разработка смарт-карт, проведение онлайн опросов, работа с агрегаторами научной литературы, разработка онлайн

тестов, использование Tor project методом включенного наблюдения, обучение навыкам использования статистических сервисов и специализированных научных платформ). Они направлены на повышение качества подготовки путем развития у студентов необходимых цифровых компетенций, связанных с осуществлением исследовательской и научной деятельности. Среди предусмотренных настоящей рабочей программой выделены следующие:

Создание интеллект-карт — это онлайн-инструмент для майндмэппинга, который позволяет захватывать, разрабатывать и делиться идеями визуально.

Задача студента: составить ментальную карту по теме «Кибервиктимология и ее место среди современных наук об обществе» на ресурсе https://www.mindmeister.com/ru

Организация и проведение социологического опроса в сети интернет при помощи специализированных социологических порталов (Анкетолог, SurveyMonkey, Яндекс.Взгляд)

Задача студента: проведение интернет-анкетирования 20-80 человек по выбранной теме, касающейся виктимизации пользователей сети (например, «Становились ли Вы жертвой интернет-мошенничества», «Частота кибербуллинга среди школьников», «Криминальная дискриминация в социальных сетях», «Ущерб, наносимый жертвам киберпреступлений» и проч.). Для этого необходимо зарегистрироваться на одном из социологических сервисов (https://anketolog.ru/, https://www.surveymonkey.ru/), выбрать пробный тариф, разработать анкету из 3–5 вопросов и разместить ее для сбора ответов. После этого обратиться к потенциальным респондентам (своим подписчикам, коллегам по работе или ВУЗу) с просьбой пройти опрос.

Визуализация информации и построение диаграмм онлайн.

Задача студента: изучить и систематизировать виды кибервиктимизации, а также отразить данную номенклатуру в диаграмме, выполненной в любом из сервисов визуализации, например, https://yequalx.com/ru/chart/

Работа с агрегаторами научных публикаций. Изучение степени разработанности той или иной научной темы, касающейся становления, поведения и особенностей интернет-жертв.

Задача студента: по ключевым словам, составить и проанализировать научные публикации по той или иной проблеме кибервиктимологии. Для этого на специализированных порталах (напр., https://www.mendeley.com, https://elibrary.ru/) выбрать нужное ключевое слово (например, кибермошенничество, интернет-сталкинг, сексуальные домогательства в сети и проч.) и систематизировать по годам список релевантной научной литературы. Это позволит выявить актуальность проблемы, проследить интенсивность ее разработки, уточнить наиболее и наименее интересующие ученых аспекты рассматриваемой темы.

Работа с интернет-сервисами статистической аналитики представляет собой подготовку доклада на свободную наиболее заинтересовавшую студента тему, касающуюся виктимизации в виртуальном пространстве.

Задача студента: по ключевому запросу (например, «cyber victim», «cyber crime») в сервисе www.statista.com выбрать наиболее интересную тему с открытым доступом, составить по ней презентацию и представить ее на семинарском занятии.

Включенное наблюдение в clearnet и deepnet

Задача студента: совместно с преподавателем проанализировать типы виктимизирующих действий по теме № 6 и найти в Клирнете или Даркнете поставщиков подобных услуг, оценить объем предложений, актуальную ценовую политику и проч.

Анализ интернет-контента.

Задача студента: провести контент-анализ публицистической, научной и иной литературы за прошедший год на предмет выявления новых видов мошеннических действий в сети Интернет (например, в 2020 г. появились новые формы таких действий: кьюшинг, COVID-мошенничества и проч.)

Разработка и создание тестов при помощи специализированных интернет-платформ.

Задача студента: разработать мини-тест (5-10 вопросов) на тему «Становились ли Вы жертвой мошеннических действий в сети Интернет?», используя инструментальный функционал онлайн платформ, например, Survio.

Целевой интернет-серфинг.

Задача студента: в сети Интернет выбрать актуальные фейковые новости, проанализировать их, дать прогноз возможных последствий подобной публикационной активности.

Организационная деятельность в интернет-пространстве.

Задача студента: малой группой совместно с преподавателем организовать и провести в сети Интернете научное мероприятие на площадке https://event.4science.ru. Тему и содержание мероприятия определить в ходе брэйнсторминга на предыдущих семинарских занятиях. Мероприятия должно включать не менее 2–3 докладов и обсуждение затронутых проблем.

Заключительная часть курса

В завершении курса предусмотрена онлайн конференция участников, тестирование и зачет. Вопросы к зачету могут быть следующими:

1. Кибервиктимология: предмет и перспективы
2. Современные кибервиктимологические исследования
3. Кибервиктимность: понятие и отличие от классической виктимности
4. Понятие и сущность кибервиктимизации
5. Модель ПОРПЭ в изучении виртуальной виктимизации
6. Виды и формы кибервиктимизации
7. Кибержертва, отличие от смежных понятий
8. Виды кибержертв
9. Поведенческие факторы кибервиктимизации
10. Психологические факторы кибервиктимизации
11. Социальные факторы кибервиктимизации
12. Технические факторы кибервиктимизации
13. Виктимологическая характеристика преступлений, связанных с повреждением сетевой инфраструктуры
14. Виктимологическая характеристика интернет-мошенничества
15. Виктимологическая характеристика феномена фейка
16. Виктимологическая характеристика кибербуллинга
17. Виктимологическая характеристика киберсталкинга
18. Виктимологическая профилактика киберпреступности
19. Индивидуальная виктимологическая профилактика в киберпространстве

Тестовые задания, представленные в рабочей программе, должны отвечать следующим требованиям: соответствовать целям обучения; отражать наиважнейшие аспекты учебного курса, быть точными, последовательными и логичными, вместе с тем, ясными для понимания, компактными [6]. Примерный материал для прохождения тестирования может включать в себя следующие задания:

1. Выберите наиболее точное определение кибервиктимологии

– наука о жертвах преступлений

– междисциплинарная область, исследующая виктимизацию пользователей в виртуальном пространстве объединенных компьютерных сетей.

– концепция, связывающая воедино криминальную и виктимную активность пользователей Интернета

2. Интегративный подход в кибервиктимологии — это

– применение комплекса социологических, криминологических, психологических, технических тактик и знаний в их необходимой совокупности

– изучение социальных связей между виртуальными жертвами и киберпреступниками

– использование общенаучных и частно-научных методов для проведения исследований

3. Предикторы (маркеры) кибервиктимизации это

– ее индивидуальные предсказатели или предуказатели

– комплекс факторов, обусловливающих данную форму поведения

– последствия становления кибержертвы

4. Какие источники используются для сбора информации об эпизодах виктимизации в киберпространстве?

– данные официальной статистики МВД и Прокуратуры

– общие, тематические отчеты органов власти, виктимологические опросы

– сведения из публицистических источников

5. Что такое имперсонация?

– выдача себя за другого человека;

– кража паролей;

– сексуальные домогательства в сети.

6. Кибервиктимность определяется как

– процесс становления жертвы преступления в виртуальной среде

– способность индивида быть жертвой компьютерных преступлений в силу субъективной или объективной уязвимости.

– психологический и моральный вред, нанесенный преступниками в интернете

7. Укажите какие из перечисленных элементов входят в предмет кибервиктимологии (допускается несколько ответов):

– жертвы преступлений в виртуальной среде

– кибервиктимность и кибервиктимизации

– история кибервиктимологии

– прогнозирование виктимного поведения в Интернете

– ситуации, предшествующие кибервиктимизации

– посткриминальное поведение жертвы

– система мероприятий профилактического характера

8. Кто такие жертвы вовлечения в кибервиктимологии?

– объекты клеветы, оскорбления, травли, киберпреследования, порно из мести, порнографических дипфейков

– лица, которых склонили к антиобщественному или опасному поведению

– потерпевшие от преступлений, направленных на причинение технического вреда

– потерпевшие от интернет-краж, мошенничеств, вымогательства денежных средств

9. Виктимная амбивалентность — это

– способность одной жертвы становиться потерпевшим от нескольких форм киберкриминального поведения

– представленность среди кибержертв тех, кто допускает противоправное и аморальное поведение, провоцируя тем самым преступления в отношении себя
– одна из психологических характеристик потерпевших в Интернете

10. Какие из представленных мотивов виктимизации юридических лиц являются ведущими?
– ибервойна
– финансовая выгода
– хактивизм
– получение информации для различных целей

11. Являются ли термины «субъект кибервиктимизации» и «кибержертва» синонимичными?
– да, являются
– нет, это абсолютно разные понятия
– субъект кибервиктимизации включает в себя понятие «кибержертвы»

12. Какие подвиды включает в себя «фейк-презентация»?
– некомпетентные советы и указания (лайфхаки)
– создание лжеэкспертов, фейковые комментарии, посты и обсуждения
– фейк как элемент хищения
– дипфейки

Представленный курс в наилучшей степени соответствует задаче формирования современных специалистов в области цифровой криминологии, киберкриминалистики и других социально-юридических наук. О необходимости решения этой задачи, о целесообразности повышения значимости цифровых технологий при решении задач уголовной политики, ученые высказывались неоднократно [7–9]. Представленный учебный предмет поможет усвоить знания об основных путях эволюции преступности, проследить качественные и количественные изменения в характеристиках потерпевших от виртуальных преступлений, приобрести необходимые научно-исследовательские навыки и опыт их практической реализации в киберсреде. Таким образом, кибервиктимология способна удовлетворить потребность в новых научно-методических исследованиях в области педагогики по проблемам подготовки к осуществлению виктимологической деятельности [10].

Список использованной литературы

1. Педагогика : учеб. пособие / под ред. П.И. Пидкасистого. — 2-е изд. — Москва : Рос. педагог. агентство, 1996. — 603 с.

2. Кириленко В.П. Киберпреступность и цифровая трансформация / В.П. Кириленко, Г.В. Алексеев // Теоретическая и прикладная юриспруденция. — 2021. — № 1 (7). — С. 39–53.

3. Серебренникова А.В. Криминологические проблемы цифрового мира (цифровая криминология) / А.В. Серебренникова. — DOI 10.17150/2500-4255.2020.14(3).423-430 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 3. — С. 423–430.

4. Лихачёв Б.Т. Педагогика: курс лекций : учеб. пособие / Б.Т. Лихачёв. — 4-е изд., перераб. и доп. — Москва : Юрайт-М, 2001. — 607 с.

5. Рышкова А. Киберпреступность в России увеличилась в 20 раз за последние 7 лет электронный ресурс / А. Рышкова // Комсомольская правда. — 2020. — 25 июля. — URL: https://www.kp.ru/online/news/3955606.

6. Ядгарова Л.Д. Требования к тестовым заданиям в электронных учебниках / Л.Д. Ядгарова, С.Б. Эргашева // Проблемы науки. — 2020. — № 8 (56). — С. 36–38.

7. Судакова Т.М. Осмысление будущего криминологии: обзор современных тенденций / Т.М. Судакова, В.А. Номоконов. — DOI 10.17150/2500-4255.2018.12(4).531-540 // Всероссийский криминологический журнал. — 2018. — Т. 12, № 4. — С. 531–540.

8. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А.П. Суходолов, С.В. Иванцов, С.В. Борисов, Б.А. Спасенников. — DOI 10.17150/2500-4255.2017.11(1).13-21 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 1. — С. 13–21.

9. Максимов С.В. Цифровая криминология как инструмент борьбы с организованной преступностью / С.В. Максимов, Ю.Г. Васин, К.А. Утаров. — DOI 10.17150/2500-4255.2018.12(4).476-484 // Всероссийский криминологический журнал. — 2018. — Т. 12, № 4. — С. 476–484.

10. Рыжова Н.И. Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности / Н.И. Рыжова, О.Н. Громова. — DOI 10.22363/2312-8631-2020-17-3-254-268 // Вестник Российского университета дружбы народов. Серия: Информатизация образования. — 2020. — Т. 17, № 3. — С. 254–268.

Информация об авторе

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, кафедра уголовного права, криминологии и уголовного процесса, Институт государства и права, Байкальский государственный университет, e-mail: zdevraz@ya.ru.

Author

Dmitry V. Zhmurov — PhD in Law, Associate Professor, Department of Criminal Law, Criminology and Criminal Procedure, Institute of State and Law, Baikal State University, Irkutsk, Russian Federation, E-mail: zdevraz@ya.ru.

Для цитирования

Жмуров Д.В. Кибервиктимология, как новая учебная дисциплина: методическая разработка / Д.В. Жмуров. — DOI 10.17150/2411-6262.2021.12(3).25 // Baikal Research Journal. — 2021. — Т. 12, № 3.

For Citation

Zhmurov D.V. Cybervictimology as a New Course Unit: Methodological Guidance. *Baikal Research Journal*, 2021, vol. 12, no. 3. DOI: 10.17150/2411-6262.2021.12(3).25. (In Russian).