RUDN Journal of Informatization in Education
Вестник РУДН. Серия: Информатизация образования
2020 Vol. 17 No. 3 254–268
http://journals.rudn.ru/
informatization-education

DOI 10.22363/2312-8631-2020-17-3-254-268
УДК 378.02:372.8:373.1.02

Научная статья

Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности

Н.И. Рыжова[1], О.Н. Громова[2]

[1]Институт управления образованием Российской академии образования
Российская Федерация, 105062, Москва, ул. Жуковского, 16
[2]Санкт-Петербургский гуманитарный университет профсоюзов
Российская Федерация, 192236, Санкт-Петербург, ул. Фучика, 15

Аннотация. *Проблема и цель.* В статье рассматриваются виктимологические признаки преступлений в сфере использования информационных технологий и киберугрозы в условиях цифровизации современного социума. Подчеркивается актуальность научно-методических исследований в области педагогики по проблемам подготовки к осуществлению виктимологической деятельности.

Методология. Исследование опирается на анализ основных вызовов цифрового социума и внутренней логики развития прикладной виктимологии как науки о противодействии развитию виктимности субъектов различных сфер жизнедеятельности человека в условиях угроз современного социума.

Результаты. В исследовании на основе анализа перечислены и охарактеризованы виды существующих киберугроз в зависимости от объекта посягательства и законодательные акты, определяющие информационную безопасность и кибербезопасность. Отмечена не только актуальность рассмотрения новых угроз информационного общества, вызывающих необходимость развития информационной безопасности и кибербезопасности как самостоятельных научных направлений информатики и отчасти прикладной виктимологической науки, но и развитие терминологического и критериального аппарата в данной области, а также формирования в системе образования профессиональной компетентности у современных специалистов в области применения профессиональных виктимологических знаний, направленных на предупреждение киберпреступлений.

Заключение. В свете потребности в профилактических мерах в рамках противодействия киберпреступности и обеспечения кибербезопасности в статье говорится о необходимости совершенствования подходов к образованию и развитию специальной составляющей в профессиональной деятельности современных субъектов разного уровня – виктимологической деятельности.

Ключевые слова: цифровизация общества, информатизация образования, информационная безопасность, киберугрозы, кибербезопасность, виктимологические признаки, виктимологическая деятельность

Постановка проблемы. Развитие современного общества в мировом масштабе всегда определяется глобальными вызовами современности. Среди них особое место занимают вызовы, связанные с развитием и внедрением цифровых технологий в различные сферы жизнедеятельности человека и современного социума, порождающие не только позитивные изменения, но и определенные угрозы для его членов [1–8], например:

– цифровизация экономических и общественных отношений (цифровая экономика, роботизация, искусственный интеллект, Интернет вещей и пр.);

– экспоненциальный рост неструктурированных данных (более 70–80 % от всех данных в организациях – неструктурированные);

– конвергенция: материальных и информационных, информационных и когнитивных технологий;

– виртуализация реальности: стирание границ между реальностью и виртуальным миром; информационная социализация; утрата чувства «необратимости жизни»; обеднение содержания реального общения между людьми и снижение эмоционального интеллекта и др.

В свою очередь, отдельно взятое государство помимо глобальных процессов подчиняется локальным изменениям, происходящим внутри страны. Сегодня любая организация собирает, обрабатывает и хранит солидные объемы информации, зачастую являющейся конфиденциальной, хищение которой способно причинить вред организации в целом и отдельно взятому человеку. С каждым годом увеличивается количество компьютеров, смартфонов, планшетов и других технических устройств (гаджетов), что обуславливает необходимость обеспечения как эффективных мер защиты информационных технологий, так и самих пользователей от неблагоприятного информационного и кибервоздействия в условиях цифровизации современного социума.

Методы исследования. Основным методами исследования обозначенной проблематики являются изучение накопленного эмпирического опыта и его обобщение, а также анализ и интерпретация существующей нормативно-правовой и законодательной базы, определяющей методы предупреждения, профилактики и пресечения негативных последствий – киберугроз, обусловленных отчасти как требованиями времени, так и влиянием научно-технических достижений, продиктованных четвертой индустриальной революции, создавшей новые «цифровые» условиях для развития современного социума.

Результаты и обсуждения. Виктимологические признаки преступлений в сфере информационных технологий указаны законодателем в нормативных документах, определяющих противоправность деяний, в частности, причинение вреда собственнику уничтожением, блокированием, модификацией либо копированием в результате неправомерного доступа к охраняемой законом компьютерной информации.

В качестве особого признака виктимологической характеристики указана материальная оценка содеянного. Остальные предложенные признаки вступают в процесс виктимизации либо путем причинения конкретного вреда (причинение тяжкого вреда) участникам отношений в сфере информационных технологий, либо создавая такую возможность.

Отдельно в качестве виктимологического признака указан вред, причиняемый критической информационной инфраструктуре Российской Федера-

ции, к субъектам которой в основном законодатель относит государственные органы, государственные учреждения, российских юридических лиц и/или индивидуальных предпринимателей. Тем не менее вредные последствия могут коснуться любого гражданина страны, поскольку способны [9. С. 7]:

– причинить вред жизни или здоровью людей;

– прекратить или нарушить функционирование объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи;

– сократить возможность доступа для получателей государственной услуги;

– затронуть вопросы внутренней и внешней политики государства;

– причинить вред экологической среде;

– ограничить обеспечение обороны страны, безопасности государства и правопорядка.

Мы назвали лишь те виктимологические признаки, которые официально закреплены в действующем уголовном законодательстве и законодательстве, обеспечивающем информационную безопасность. Помимо этого, существует множество угроз, которые не указаны в качестве виктимологических признаков, но способны причинить серьезный ущерб и в первую очередь детям. Данный факт подтверждается классификацией конкретных видов угроз в зависимости от объектов посягательства (см. таблицу), представленных А. Михайловой [10].

Таблица

Виды киберугроз в зависимости от объектов посягательства [10]

Объекты киберугроз	Виды киберугроз в зависимости от объектов посягательства в условиях становления цифрового социума
Граждане	Утечка и обнародование частной информации, мошенничество, распространение опасного контента, воздействие на личность путем сбора персональных данных и атаки на инфраструктуру, используемую гражданами в обычной жизни
Бизнес	Воздействие на системы интернет-банкинга, блокирование систем покупки билетов, онлайн-торговли, геоинформационных систем и хакерские атаки на частные сайты
Государство	Атаки на ключевые государственные системы управления (электронное правительство, сайты госорганов), экономическая блокада (масштабное отключение платежных систем, систем бронирования), аппаратная атака на персональные компьютеры, смартфоны граждан и организаций, атаки на бытовые объекты, которые управляются с помощью информационно-коммуникационных технологий, и критически важную инфраструктуру

В 2016 г. Институтом современных медиа (MOMRI) были проведены серьезные исследования использования детских мобильных игр и развивающихся приложений. По данным исследования более 71 % детей в возрасте от 3 до 10 лет увлекаются играми и пользуются обучающими приложениями на смартфонах и планшетах. При этом в 49 % случаев дети начинают играть в 3–4 года, 75 % – в 5–8 лет, 84 % – 9–10 лет. Не вызывает удивления и тот факт, что к 10 годам 91 % детей мегаполиса имеют личный гаджет, так как наличие какого-либо устройства зафиксировано примерно у 25 % детей в возрасте 3–4 лет [11].

Несмотря на то что современные угрозы информационной безопасности принято характеризовать с применением приставки «кибер-», сегодня в

Российской Федерации отсутствует документ, способный обозначить фундаментальные подходы к обеспечению кибербезопасности. Соответственно, также отсутствуют базовые понятия, отграничивающие кибербезопасность от информационной безопасности. Также на уровне национального законодательства в Российской Федерации отсутствует нормативный правовой акт, содержащий необходимый понятийный аппарат и способствующий обеспечению системы безопасности в киберпространстве.

Весьма полезными документами для разработки нормативных правовых актов по обеспечению кибербезопасности являются резолюции Генеральной Ассамблеей ООН по вопросам кибербезопасности, например, «О создании глобальной культуры кибербезопасности и оценке национальных усилий по защите важнейших информационных инфраструктур», а также международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (далее – Стандарт) и др.

Достаточно подробно положения Стандарта проанализировали А.С. Марков и В.Л. Цирлов в своей работе «Руководящие указания по кибербезопасности в контексте ISO 27032» [5; 12], где обратили внимание и провели «аналогию понятия “кибербезопасность” с классическим определением информационной безопасности, но в определенной среде – киберпространстве» [13]. По их мнению, кибербезопасность следует «обязательно соотносить с конкретным субъектом и определять фактически как свойство защищенности активов субъекта от угроз конфиденциальности, целостности, доступности» [14].

Мы же заметим, обобщая существующие взгляды многих ученых, что понятие «киберпространство» сегодня все же чаще всего трактуют как комплексную среду, не существующую в физической форме, являющуюся фактически виртуальной и представляющую собой результат действий людей, программ и услуг, предоставляемых в сети Интернет с помощью различных технологических устройств и коммуникационных технологий.

Полное же определение понятия «информационная безопасность», согласно Доктрине информационной безопасности в Российской Федерации, включает в себя следующие признаки: «состояние защищенности личности, общества, государства от информационных угроз внешнего и внутреннего характера, способного обеспечить реализацию конституционных прав и свобод человека и гражданина, качество и уровень жизни, достойные каждого гражданина, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие РФ, обороноспособность и безопасность государства» [15].

Кроме утвержденной Доктрины, где дается определение информационной безопасности, существуют и действуют в нашей стране еще и следующие законодательные акты, фиксирующие и конкретизирующие определение данного понятия или его составляющих. К ним относятся:

– Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 02.12.2019 г.) «Об информации, информационных технологиях и о защите информации»;

– Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 г. № Пр-1753);

– Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– Указ Президента РФ от 09.05.2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Что же касается непосредственно безопасности киберпространства, то здесь следует отметить такие нормативные документы, как:

– Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указ Президента РФ от 15.01.2013 г. № 31 в (ред. от 22.12.2017 г.) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Совершенствование правового регулирования кибербезопасности является актуальнейшей задачей законодателя. Очевидно, что приставка «кибер-» требует от законодателя своего понятийного аппарата. Поэтому в 2013 г. на обсуждение поступил проект Концепции Стратегии кибербезопасности Российской Федерации [16], редакция которой активно критикуется различными авторами и сегодня.

Например, К.Ю. Чугунова в своей работе «Информационное оружие как угроза национальной безопасности Российской Федерации» считает, что «проект этот неоднозначен, о чем свидетельствует уже его название Концепция стратегии», и отмечает «недостаток существующего правового регулирования киберпространства как особого элемента, принимая во внимание комплексный характер проблемы и ее масштаб» [17].

Тем не менее важно отметить, что в Концепции отражена актуальность принятия программного документа в связи с проникновением информационно-коммуникационных технологий, в том числе и цифровых, во все сферы жизнедеятельности современного человека в условиях становления цифрового общества. При этом указывается, что значительный рост возможностей данного вида технологий способствует возникновению новых форм угроз, способных нарушить как права и интересы субъектов, так и причинить ущерб жизнедеятельности личности, организации, государственным органам.

Кроме того, угрозы, связанные с информационно-коммуникационными и цифровыми технологиями, подразумевают и возможности проведения кибератак киберпреступниками и кибертеррористами против защищенных информационных ресурсов, а также, возможно, в широком смысле и использование кибероружия при проведении специальных операций в контексте информационных или даже кибервойн.

Изучая содержание Концепции Стратегии кибербезопасности Российской Федерации, следует особо отметить, что ее авторами предпринята попытка наделить новые угрозы информационной безопасности (или киберугрозы) соответствующим терминологическим арсеналом, в частности, определены понятия [18]:

1) «киберпространства как сферы деятельности в информационном пространстве, образованной совокупностью коммуникационных каналов Интернета и иных телекоммуникационных сетей, технологической инфраструкту-

ры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности;

2) кибербезопасности как совокупности условий, позволяющих защитить киберпространство от угроз и воздействий с отрицательными последствиями».

Эти отрицательные последствия характеризуют общественную опасность и противоправность деяний, которые все чаще в своей совокупности называют киберпреступностью, являющейся новой криминальной угрозой в киберпространстве. В связи с этим возникает необходимость определения и такого понятия как «киберпреступление».

Согласно указанным выше законодательным актам и нормативным документам, киберпреступление следует трактовать как «общественное опасное, противоправное, виновное деяние, совершенное в электронной сфере при помощи компьютерных систем или сети либо против них» [14]. К особенностям данного вида преступлений целесообразно относить:

– их скрытость в связи с применением различных механизмов анонимности и шифрования;

– трансграничность, поскольку преступник и жертва могут быть разделены тысячами километров;

– наличие границ нескольких государств;

– нестандартность способов совершения;

– автоматизированность режима.

Ответственность за киберпреступления предусмотрена в гл. 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», а именно:

– за незаконное ознакомление лицом, не имеющим соответствующего доступа, с информацией, содержащейся на машинных носителях;

– за создание, использование и распространение программ, нарушающих функционирование других программ, созданных или принадлежащих добросовестным пользователям;

– за нарушение установленных правил, повлекшее причинение крупного ущерба обладателю информационного ресурса.

Крое того, к преступлениям в сфере компьютерной информации относятся противоправные деяния, совершенные способом хищения с использованием электронных средств доступа: мошенничество, то есть деяние, совершенное путем незаконного использования платежных карт, а также путем технического проникновения в платежные системы кредитных и иных финансовых организаций.

Примечательно, что и Уголовный кодекс РФ не содержит определения понятий с приставкой «кибер-», ограничиваясь такой категорией как «компьютерная информация», под которой понимаются «…сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» (Примечание к ст. 272 УК РФ).

Стремительное формирование единого глобального информационного пространства, обострение цифрового неравенства, создание потенциала для подрыва национальной безопасности, нарушение общественного и государственного порядка, неготовность к массовому применению технологий вир-

туальной реальности, отсутствие эффективной защиты личной жизни и личного жизненного пространства порождают серьезные угрозы для всего населения России [19].

Ускоренный рост компьютеризации, считают ученые, сопровождается прогрессирующим ростом киберугроз, порождающих все новые формы киберпреступности, которая в немалой степени затрагивает интересы детей и молодежи (что подтверждается эмпирическим психодиагностическим исследованием молодежи). В связи с чем предлагается актуализировать исследование «причин кибервиктимизации молодежи, изучение индивидуально-личностных особенностей кибержертв, психологических механизмов становления кибервиктимного поведения пользователей киберпространства, поиск путей обеспечения кибербезопасности представителей молодежной среды» [20].

Учитывая сказанное и существующий психолого-педагогический опыт, в рамках воспрепятствования становления кибервиктимного поведения молодежи необходимо усилить социально-психологическое направление профилактики данного вида виктимности путем разработки и внедрения комплекса мероприятий, направленных на формирование, развитие либо коррекцию личностно-индивидуальных качеств поведения.

Отмечая необходимость профилактики киберэкстремизма в системе высшей школы, Г.Н. Чусавитина и Н.Н. Зеркина указывают на молодежь, как «наиболее уязвимую часть населения для идей насильственного экстремизма, ксенофобии, нетерпимости и террористической радикализации» [21]. В связи с этим основной и крайне актуальной целью своих методических исследований многие авторы считают сегодня разработку и апробацию специальных методик в контексте профессиональной подготовки студентов педагогических специальностей в условиях университетов к профилактике и противодействию идеологии киберэкстремизма среди детей, подростков и молодежи [4; 5; 22–24].

Д.Н. Карпова предлагает «в качестве мер противодействия киберпреступности и интернет-зависимости выработку правовых норм регулирования Интернета» [24].

Помимо преступности в киберпространстве наблюдаются такие угрозы и деструктивные проявления, как киберагрессия в виде троллинга, кибербуллинга/кибермоббинга и астротурфинга. В этих условиях в основном предлагается проведение профилактических мероприятий, направленных на превенцию киберагрессии в интернет-пространстве и, соответственно, на предотвращение противоправных проявлений в отношении детей. По сути, все авторы, обсуждая проблемы кибербезопасности, предлагают проводить некие профилактические меры. При всей справедливости этих предложений, на наш взгляд, для решения такой глобальной проблемы, как предупреждение противоправного поведения в киберпространстве, при наличии многочисленного и неопределенного субъектного состава требуется целенаправленная, методически и нормативно обеспеченная систематическая *виктимологическая деятельность.*

Необходимо отметить, что проведенные нами ранее исследования предмета виктимологии обозначили проблему, указывающую на то, что современ-

ная наука не содержит единого представления о его содержании [12; 22; 23; 25–27;], а современные исследователи настаивают на том, что виктимология по-прежнему изучает исключительно только жертв как криминальных, так и не связанных с преступной деятельностью. При этом становление виктимологической науки в этом качестве, хотя и несколько стихийно, но происходит на современном этапе формирования цифрового общества и под влиянием угроз, им же и спровоцированным.

Наше представление о предмете виктимологии с позиций ее онтологического развития вносит серьезные изменения и в трактовку самой науки, и в ее содержание, порождая новые прикладные виды виктимологии (например, кибервиктимология, экологическая виктимология, виктимология катастроф и др.).

На наш взгляд, помимо исследования жертвы как таковой (узкое понимание виктимологии как науки – фундаментальный взгляд, гносеологический подход), для современной науки важно и необходимо изучать в первую очередь угрозы современного социума, а затем уже механизмы противодействия развитию виктимности субъектов различных сфер жизнедеятельности человека в условиях этих угроз, и предлагать методы профилактики самих угроз (в этом заключается трактовка виктимологии в широком смысле – прикладном, онтологическом).

При этом именно в рамках методологии данной науки – посредством деятельности, условно называемой «виктимологической», – должны осуществляться как предотвращение процессов виктимизации субъектов разного уровня, так и разработка специальных методов, приемов и технологий предупреждения процессов виктимизации субъектов, учитывающих потенциальные и реальные угрозы современного социума (в том числе и киберугрозы).

Таким образом, *виктимологическая деятельность* – это ни что иное, как деятельность государственных органов, общественных объединений, юридических и физических лиц, в компетенцию которых включена обязанность:

– способствовать девиктимизации и виктимологическому противодействию преступности;

– устранению потенциальных и реальных угроз;

– обеспечению национальной, информационной, кибербезопасности, в том числе на законодательном и организационном уровнях.

Рассматривая ранее и достаточно подробно актуальность виктимологической деятельности и ее особенности, мы пришли к заключению, что осуществлять ее должны государственные органы, учреждения и организации, а также физические и юридические лица, уполномоченные законодательством обеспечивать, например, кибербезопасность. При этом они должны осознавать, что это «особый вид социальной деятельности, осуществляемой в условиях сознательной и мотивированной направленности на удовлетворение общесоциальных потребностей и ориентированной на достижение конечной цели, заключающейся в защите от противоправных посягательств, осуществляемой субъектами посредством определенных форм и средствами, одобряемыми государством» [27. С. 11]. В данном контексте также важно понимать, что основными задачами виктимологической деятельности являются

обеспечение защищенности личности и общества от любых угроз и виктимизации, а также их последствий; восприятие уровня такой защищенности обществом и его членами; достижение оптимального на данном этапе уровня защищенности интересов личности и общества от воздействия виктимогенных детерминантов и т. п.

Сознательную и мотивированную направленность на осуществление виктимологической деятельности в области кибербезопасности порождают потребности, формирующие осознание обществом необходимости принятия социально значимых мер, направленных на противодействие киберпреступности и другим противоправным проявлениям в киберпространстве.

Заключение. Подытоживая сказанное, отметим, что реализация указанных потребностей должна происходить, по нашему мнению, посредством следующих мероприятий и средств, которые были обозначены нами ранее в публикациях [12; 22–27], но уже с учетом особенностей и условий, диктуемых киберпространством [25]:

– «проведения фундаментальных научных исследований, позволяющих получить новые знания о возможностях виктимологической профилактики и защиты, способных обеспечить формирование правосознания на основе субъективных ценностных отношений, восприятие правовых норм как неотъемлемую обязанность к определенному поведению, создание законодательной и финансовой базы в целях проведения мероприятий, обеспечивающих оздоровление материального положения потерпевшей стороны, обеспечивая тем самым безопасность личности, общества и государства;

– правового обеспечения, выражающегося в формировании системы нормативных актов, содержащих положения о защите жертв преступных посягательств киберпреступности и других киберправонарушений;

– реализации совместных (с участием зарубежных партнеров) программ, связанных с виктимологической профилактикой и защитой жертв киберпреступности и других киберправонарушений;

– содействия деятельности общественных и образовательных организаций, в том числе повышения их статуса;

– распространения научных и правовых виктимологических знаний в области киберпреступности и других киберправонарушений;

– формирования специальной профессиональной компетентности у современных специалистов (например, юристов, педагогов, специалистов в сфере информационных технологий и др.) в области применения профессиональных виктимологических знаний, направленных на предупреждение киберпреступлений и других киберправонарушений».

В заключение отметим, что в данном контексте особую актуальность приобретает и проблематика научно-методических исследований в области педагогики и психологии по вопросам подготовки к осуществлению «виктимологической деятельности субъектами учебно-воспитательного процесса как составляющих обеспечения безопасности жизнедеятельности детей в современном социуме» [22].

При этом, с нашей точки зрения, отдельного внимания в контексте виктимологической профилактики и защиты, осуществляемых субъектами учебно-

воспитательного процесса на разных его уровнях, заслуживают вопросы кибербезопасности детей и подростков, на которые указывает в Концепции информационной безопасности детей и подростков (2013 г.) один из ее разработчиков – доктор психологических наук, профессор МГУ имени М.В. Ломоносова О.А. Карабанова [4]. Перечислим эти риски для воспитания и развития подрастающего поколения в современном обществе, способные вызывать определенные деформации личности в информационной и виртуальной среде, которым сегодня уже уделяется особое внимание в научно-педагогических публикациях [4; 5]:

– «межкультурные и этнокультурные риски – ксенофобия, мигрантофобия, этноизоляционизм;

– риски информационной социализации и низкий уровень безопасности информационной среды для детей и подростков;

– риски трудности жизненного, профессионального и ценностного самоопределения;

– риски десоциализации, агрессии, отклоняющегося поведения и аддикций, эскапизма;

– риски вовлечения подростков в группы экстремистской направленности и др.».

Таким образом, новое время и новые цифровые технологии предоставляют каждому из нас как новые формы общения и новые возможности, так и новые риски, связанные с цифровизацией, влияющие на нашу информационную и кибербезопасность в условиях становления цифрового социума.

Поиск новых концепций и выявление новых методических подходов как для обеспечения информационной безопасности личности, так и для противодействия негативным последствиям, профилактики киберугроз, вызванных современными условиями цифровизации и становлением цифрового общества, невозможны без осмысления и понимания сути как положительных, так и отрицательных сторон этих процессов.

Благодарности и финансирование. Работа выполнена в рамках государственного задания № 2.9384.2017/БЧ «Развитие информатизации образования в контексте информационной безопасности личности».

Список литературы

[1] *Бешенков С.А., Миндзаева Э.В., Шутикова М.И.* Информационная безопасность в контексте вызовов цифрового социума // Человек и образование. 2018. № 2 (55). С. 55–61.

[2] *Бешенков С.А., Шутикова М.И., Рыжова Н.И.* Формирование содержания курса информатики в контексте обеспечения информационной безопасности личности // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2019. Т. 16. № 2. С. 128–137.

[3] *Гриншкун В.В.* Особенности подготовки педагогов в области информатизации образования // Информатика и образование. 2011. № 5 (223). С. 68–72.

[4] *Карабанова О.А., Молчанов С.В.* Риски негативного воздействия информационной продукции на психическое развитие и поведение детей и подростков // Национальный психологический журнал. 2018. № 3 (31). С. 37–46.

[5] *Козлова Е.Б.* Профилактика деформаций личности в информационной и виртуальной среде // Научные труды Калужского государственного университета имени К.Э. Циол-

ковского: материалы докладов психолого-педагогических секций региональной университетской научно-практической конференции. Калуга, 2018. С. 423–431.

[6] *Литвиненко М.В.* Информационная безопасность и реформы в сфере образования // Приложение к журналу «Известия вузов. Геодезия и аэрофотосъемка». 2009. № 2–1. С. 194–197.

[7] *Лубков А.В., Каракозов С.Д., Рыжова Н.И.* Тенденции развития современного образования в условиях становления цифровой экономики // Информатизация образования: теория и практика: материалы международной научно-практической конференции. Омск: ОмГПУ, 2017. С. 41–47.

[8] *Karakozov S.D., Ryzhova N.I.* Information and education systems in the context of digitalization of education // Journal of Siberian Federal University. Humanities & Social Sciences. 2019. No. 12(9). Pp. 1635–1647. http://doi.org/0.17516/1997–1370–0485.

[9] Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. № 167. 2017, 31 июля.

[10] Проблемы кибербезопасности в России и пути их решения // Гарант.ру. URL: https://www.garant.ru/article/520694/ (дата обращения: 20.03.2020).

[11] Более 70 % детей в крупных городах играют на планшетах и смартфонах. URL: https://life.ru/p/943048/ (дата обращения: 20.03.2020).

[12] Критерии оценки состояния информационной безопасности детей и подростков. URL: https://rkn.gov.ru/docs/Razdel_5.pdf (дата обращения: 20.03.2020).

[13] *Марков А.С., Цирлов В.Л.* Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28–35.

[14] *Цирлов В.Л.* Правовые основы кибербезопасности Российской Федерации. 2013. URL: https://cyberleninka.ru/article/n/pravovye-osnovy-kiberbezopasnosti-rossiyskoy-federatsii-1/viewer (дата обращения: 14.04.2020).

[15] Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

[16] Проект Концепции Стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 20.03.2020).

[17] *Чугунова К.Ю.* Информационное оружие как угроза национальной безопасности Российской Федерации // Актуальные проблемы российского права. 2015. № 7. С. 59–64.

[18] Прогноз научно-технологического развития Российской Федерации на период до 2030 года (утв. Правительством РФ) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_157978/ (дата обращения: 20.03.2020).

[19] *Бовть О.Б., Семенова Е.В.* Исследование кибервиктимного поведения молодежи и направления обеспечения кибербезопасости // Управление в условиях глобальных мировых трансформаций: экономика, политика, право: материалы научно-практической конференции. Севастополь: Рибест, 2019. С. 466–468.

[20] *Чусавитина Г.Н., Зеркина Н.Н.* Профилактика киберэкстремизма в системе современной высшей школы как социальная проблема // Мир науки. Социология, филология, культурология. 2016. № 1. С. 2.

[21] *Карпова Д.Н.* Интернет-коммуникация: новые вызовы для молодежи // Вестник МГИМО-Университета. 2013. № 5 (32). С. 208–212.

[22] *Громова О.Н.* Виктимологическая деятельность как основа профессиональной виктимологической компетентности будущего специалиста для экономической сферы // Современные проблемы науки и образования. 2015. № 3. С. 452.

[23] *Рыжова Н.И., Громова О.Н.* Актуальность виктимологической деятельности субъектов учебно-воспитательного процесса как составляющая обеспечения безопасности жизнедеятельности детей в современном социуме // Организационно-правовое регулирование безопасности жизнедеятельности в современном мире: материалы II Международной научно-практической конференции. СПб., 2018. С. 40–46.

[24] *Рыжова Н.И., Громова О.Н., Башмакова Н.И.* Медиация как актуальная составляющая виктимологической деятельности современного специалиста в условиях вызовов современности // Вопросы современной науки и практики. Университет имени В.И. Вернадского. 2017. № 4 (66). С. 181–193.
[25] *Громова О.Н.* Виктимологическая деятельность как составляющая профессионально-правовой деятельности специалистов по обеспечению экономической безопасности субъектов малого и среднего бизнеса // Мир науки, культуры, образования. 2015. № 3 (52). С. 34–39.
[26] *Громова О.Н., Рыжова Н.И.* Виктимологическая профилактика и защита как основа профессиональной виктимологической подготовки специалистов для новой экономики // Мир науки, культуры, образования. 2015. № 1 (50). С. 8–13.
[27] *Громова О.Н., Рыжова Н.И.* Критерии профессиональной готовности специалиста экономической сферы к виктимологической деятельности // Современные проблемы науки и образования. 2016. № 6. С. 480.

История статьи:
Дата поступления в редакцию: 10 марта 2020 г.
Дата принятия к печати: 13 апреля 2020 г.

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

Сведения об авторах:
Рыжова Наталья Ивановна, доктор педагогических наук, профессор, главный научный сотрудник Центра информатизации образования Института управления образованием Российской академии образования. E-mail: nata-rizhova@mail.ru

Громова Ольга Николаевна, кандидат юридических наук, доцент, заведующая кафедрой отраслей права Санкт-Петербургского гуманитарного университета профсоюзов. E-mail: oritus@yandex.ru

DOI 10.22363/2312-8631-2020-17-3-254-268

Scientific article

Cyber treats of digital society and their prevention in the context of victimological activities

Natalia I. Ryzhova[1], Olga N. Gromova[2]

[1]Institute of Education Management of the Russian Academy of Education
16 Zhukovskogo St, Moscow, 119121, Russian Federation
[2]Saint Petersburg Humanitarian University of Trade Unions
15 Fuchika St, Saint Petersburg, 192236, Russian Federation

Abstract. *Problem and goal.* The article discusses the victimological signs of crimes in the field of using information technology and cyber threats in the context of digitalization of modern society. The relevance of scientific and methodological research in the field of peda-

gogy on the problems of preparation for the implementation of victimological activities is emphasized.

Methodology. The study is based on the analysis of major challenges of digital society and the internal logic of the development of applied victimology, which is mainly concerned with preventing victimization amid the threats to modern society.

Results. Based on the analysis, the study lists and describes the types of existing cyber threats depending on the object of the attack, as well as legislative acts that define information security and cybersecurity. It is noted not only the relevance of considering new threats to the information society, which cause the need for the development of information security and cybersecurity as independent scientific areas of informatics and partly applied victimology, but also the development of terminology and criteria in this area, as well as the formation of professional competence in the education system of modern specialists in the field of professional victimological knowledge aimed at preventing cybercrime.

Conclusion. To prevent cybercrimes and to ensure cybersecurity, victimological activities, a special component in the professional activities of modern subjects of different levels, should be developed and carried out.

Keywords: digitalization of society, informatization of education, information security, cyber threats, cybersecurity, victimological signs, victimological activities

Acknowledgements and Funding. The work was performed in the framework of state task No. 2.9384.2017/BCH "Development of Informatization of Education in the Context of Personal Information Security".

References

[1] Beshenkov SA, Mindzaeva EV, Shutikova MI. Informacionnaya bezopasnost' v kontekste vyzovov cifrovogo sociuma [Information security in the context of the challenges of the digital society]. *Chelovek i obrazovanie* [*Man and education*]. 2018;2(55):55–61.

[2] Beshenkov SA, Shutikova MI, Ryzhova NI. Formirovanie soderzhanija kursa informatiki v kontekste obespechenija informacionnoj bezopasnosti lichnosti [The formation of course content of computer science in the context of ensuring personal information security]. *Bulletin of Peoples' Friendship University of Russia. Series: Informatization in Education*. 2019;16(2):128–137.

[3] Grinshkun VV. Osobennosti podgotovki uchiteley v sfere informatizatsii obrazovaniya [Features of teacher training in the field of informatization of education]. *Informatika i obrazovaniye* [*Computer Science and Education*]. 2011;5(223):68–72.

[4] Karabanova OA, Molchanov SV. Riski negativnogo vozdejstviya informacionnoj produkcii na psixicheskoe razvitie i povedenie detej i podrostkov [Risks of negative impact of information products on mental development and behavior of children and adolescents]. *Nacionalnyj psixologicheskij zhurnal* [*National Psychological Journal*]. 2018;3(31):37–46.

[5] Kozlova EB. Profilaktika deformatsiy lichnosti v informatsionnoy i virtual'noy srede [Prevention of personality deformations in the information and virtual environment]. *Nauchnyye trudy Kaluzhskogo gosudarstvennogo universiteta imeni K.E. Tsiolkovskogo* [*Scientific works of Kaluga State University named after K.E. Tsiolkovsky*]: materials of reports of psychological and pedagogical sections of the regional university scientific and practical conference (p. 431). Kaluga; 2018.

[6] Litvinenko MV. Informacionnaya bezopasnost i reformy v sfere obrazovaniya [Information security and educational reforms]. *Prilozhenie k zhurnalu Izvestiya vuzov. Geodeziya i aerofotosemka* [*Appendix to the journal Izvestiya vuzov. Geodesy and aerial photography*]. 2009;(2–1):194–197.

[7] Lubkov AV, Karakozov SD, Ryzhova NI. Tendencii razvitiya sovremennogo obrazovaniya v usloviyah stanovleniya cifrovoi ekonomiki [Trends in the development of modern education in the conditions of the digital economy]. *Informatizaciya obrazovaniya:*

teoriya i praktika [*Informatization of education: theory and practice*]: materials of the international scientific and practical conference (pp. 41–47). Omsk: OmGPU Publ.; 2017.

[8] Karakozov SD, Ryzhova NI. Information and education systems in the context of digitalization of education. *Journal of Siberian Federal University. Humanities & Social Sciences.* 2020;12(9):1635–1647. http://doi. org/0.17516/1997–1370–0485

[9] Federalnyj zakon ot 26.07.2017 No. 187-FZ "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii" [Federal Law of July 26, 2017, No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation"]. *Rossijskaya gazeta* [*Russian newspaper*]. 2017, July 31. No. 167.

[10] Problemy kiberbezopasnosti v Rossii i puti ix resheniya [Cybersecurity problems in Russia and ways to solve them]. *Garant.ru*. Available from: https://www.garant.ru/article/520694/ (accessed: 20.03.2020).

[11] *Bolee 70 % detej v krupnyx gorodax igrayut na planshetax i smartfonax* [*More than 70% of children in major cities play on tablets and smartphones*]. Available from: https://life.ru/p/943048/ (accessed: 20.03.2020).

[12] *Kriterii ocenki sostoyaniya informacionnoj bezopasnosti detej i podrostkov* [*Criteria for Assessing the State of Child and Adolescent Information Security*]. Available from: https://rkn.gov.ru/docs/Razdel_5.pdf (accessed: 20.03.2020).

[13] Markov AS, Cirlov VL. Rukovodyashhie ukazaniya po kiberbezopasnosti v kontekste ISO 27032 [Guidelines for cybersecurity in the context of ISO 27032]. *Voprosy kiberbezopasnosti* [*Cybersecurity issues*]. 2014;1(2):28–35.

[14] Cirlov VL. *Pravovye osnovy kiberbezopasnosti Rossijskoj Federacii* [*Legal basis for cybersecurity in the Russian Federation*]. Available from: https://cyberleninka.ru/article/n/pravovye-osnovy-kiberbezopasnosti-rossiyskoy-federatsii-1/viewer (accessed: 14.04.2020).

[15] Ukaz Prezidenta RF ot 05.12.2016 No. 646 "Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii" [Decree of the President of the Russian Federation of December 5, 2016, No. 646 "On approval of the Doctrine of Information Security of the Russian Federation"]. *Sobranie zakonodatelstva RF* [*Collection of the legislation of the Russian Federation*. December 12, 2016. No. 50. St. 7074.

[16] *Proekt Koncepcii Strategii kiberbezopasnosti Rossijskoj Federacii* [*Draft Concept of the Cyber Security Strategy of the Russian Federation*]. Available from: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. (accessed: 20.03.2020).

[17] Chugunova KYu. Informacionnoe oruzhie kak ugroza nacional'noj bezopasnosti Rossijskoj Federacii [Information weapons as a threat to the national security of the Russian Federation]. *Aktual'nye problemy rossijskogo prava* [*Current problems of Russian law*]. 2015;(7):59–64.

[18] Prognoz nauchno-texnologicheskogo razvitiya Rossijskoj Federacii na period do 2030 goda (utv. Pravitelstvom RF) [Forecast of the scientific and technological development of the Russian Federation for the period until 2030 (approved by the Government of the Russian Federation)]. *ConcultantPlus*. Available from: http://www.consultant.ru/document/cons_doc_LAW_157978/ (accessed: 20.03.2020).

[19] Bovt OB, Semenova EV. Issledovanie kiberviktimnogo povedeniya molodezhi i napravleniya obespecheniya kiberbezopasosti [The study cybervictims behaviour of young people and directions of cybersecurity]. *Upravlenie v uslovijah global'nyh mirovyh transformacij: jekonomika, politika, pravo* [*Management in the conditions of the global world transformations: economics, politics, law*]: scientific and practical conference (pp. 466–468). Sevastopol: Ribest Publ.; 2019.

[20] Chusavitina GN, Zerkina NN. Profilaktika kiberekstremizma v sisteme sovremennoj vysshej shkoly kak socialnaya problema [Prevention of kiberekstremizma in the modern system of higher school as a social problem]. *Mir nauki. Sociologiya, filologiya, kulturologiya* [*World of Science. Series: Sociology, Philology, Cultural Studies*]. 2016;(1):2.

[21] Karpova DN. Internet-kommunikaciya: novye vyzovy dlya molodezhi [Internet communication: new challenges for the youth]. *Vestnik MGIMO Universiteta* [*MGIMO Review of International Relations*]. 2013;5(32):208–212.

[22] Gromova ON. Viktimologicheskaya deyatel'nost' kak osnova professional'noy viktimologicheskoy kompetentnosti budushchego spetsialista dlya ekonomicheskoy sfery [Victim activity as the basis of the professional victimization of competence of the future specialist in the economic realm]. *Sovremennye problemy nauki i obrazovaniya* [*Modern problems of science and education*]. 2015;(3):452.

[23] Ryzhova NI, Gromova ON. Aktual'nost' viktimologicheskoj deyatel'nosti sub"ektov uchebno-vospitatel'nogo processa kak sostavlyayushchaya obespecheniya bezopasnosti zhiznedeyatel'nosti detej v sovremennom sociume [Relevance of victimological activity of subjects of the educational process as a component of ensuring the safety of children's life in modern society]. *Organizacionno-pravovoe regulirovanie bezopasnosti zhiznedeyatel'nosti v sovremennom mire* [*Organizational and legal regulation of life safety in the modern world*]: materials of the II International scientific and practical conference (pp. 40–46). Saint Petersburg; 2018.

[24] Ryzhova NI, Gromova ON, Bashmakova NI. Mediatsiya kak aktual'naya sostavlyayushchaya viktimologicheskoy deyatel'nosti sovremennogo spetsialista v usloviyakh vyzovov sovremennosti [Mediation as an Important Component of Victimological Activity of Modern Specialist in Conditions of Today's Challenges]. *Voprosy sovremennoj nauki i praktiki. Universitet imeni V.I. Vernadskogo* [*Problems of Contemporary Science and Practice. Vernadsky University*]. 2017;4(66):181–193.

[25] Gromova ON. Viktimologicheskaya deyatel'nost' kak sostavlyayushchaya professional'no-pravovoy deyatel'nosti spetsialistov po obespecheniyu ekonomicheskoy bezopasnosti sub"yektov malogo i srednego biznesa [Victimological activity as a component of the professional legal activity of specialists in ensuring the economic security of small and medium-sized businesses]. *Mir nauki, kultury, obrazovaniya* [*The world of science, culture and education*]. 2015;3(52):34–39.

[26] Gromova ON, Ryzhova NI. Viktimologicheskaya profilaktika i zashhita kak osnova professionalnoj viktimologicheskoj podgotovki specialistov dlya novoj ekonomiki [Victimological prevention and protection as a basis for professional victimological training for the new economy]. *Mir nauki, kultury, obrazovaniya* [*The world of science, culture and education*]. 2015;1(50):8–13.

[27] Gromova ON, Ryzhova NI. Kriterii professionalnoj gotovnosti specialista ekonomicheskoj sfery k viktimologicheskoj deyatelnosti [Criteria of professional readiness of the expert economic sphere to victim activity]. *Sovremennye problemy nauki i obrazovaniya* [*Modern problems of science and education*]. 2016;(6):480.

Article history:
Received: 10 March 2020
Accepted: 13 April 2020

For citation:
Ryzhova NI, Gromova ON. Cyber treats of digital society and their prevention in the context of victimological activities. *RUDN Journal of Informatization in Education.* 2020; 17(3):254–268. (In Russ.) http://dx.doi.org/10.22363/2312-8631-2020-17-3-254-268

Bio notes:

Natalia I. Ryzhova, doctor of pedagogical sciences, full professor, chief research officer of the center for informatization of education of the Institute of Education Management of the Russian Academy of Education. E-mail: nata-rizhova@mail.ru

Olga N. Gromova, candidate of law, associate professor, head of the department of branches of law of the Saint Petersburg Humanitarian University of Trade Unions. E-mail: oritus@yandex.ru