Право и политика
Правильная ссылка на статью:
Хамидуллин Р.С., Чуб Д.С. — Политика кибербезопасности современного образования // Право и политика. – 2023. – № 4. DOI: 10.7256/2454-0706.2023.4.39997 EDN: YMIZDD URL: https://nbpublish.com/library_read_article.php?id=39997

Политика кибербезопасности современного образования

Хамидуллин Руслан Сибагатуллович

кандидат юридических наук

начальник кафедры оперативно-разыскной деятельности органов внутренних дел, Уральский юридический институт МВД России

620072, Россия, Свердловская область, г. Екатеринбург, ул. Сыромолотова, 7

sledgsugu@mail.ru

Чуб Дмитрий Сергеевич

соискатель, кафедра оперативно-разыскной деятельности органов внутренних дел, Уральский юридический институт МВД России

620057, Россия, Свердловская область, г. Екатеринбург, ул. Корепина, 66

dima.chub2000@mail.ru

Статья из рубрики "Общественные коммуникации"

DOI:

10.7256/2454-0706.2023.4.39997

EDN:

YMIZDD

Дата направления статьи в редакцию:

18-03-2023

Аннотация: Предметом исследования является деятельность правоохранительных органов в борьбе с киберпреступностью. Объектом исследования выступают общественные отношения, возникающие в сфере образования в ходе реализации программы по борьбе с киберпреступностью в России. Автор рассматривает вопросы преступлений совершенных с помощью информационных технологий или в киберпространстве, а также организацию противодействия их совершению, деятельность, направленную на охрану здоровья граждан, обеспечение государственной и общественной безопасности. Изучает процесс использования современных способов и методов в выявлении, раскрытии преступлений совершаемых с использованием информационно-телекоммуникационных технологий. Особое внимание уделяется стратегии цифровой трансформации образования школьников и студентов: по

которой обучающиеся в рамках занятий смогут овладевать знаниями необходимыми для защиты себя и своих данных при работе техническими средствами связи. Новизна состоит в том, что прорабатываемый путь решения проблемы растущей преступности в информационной среде и преступности с использованием современных технологий напрямую влияет на современные процессы образования школьников и студентов, которые в последующем должны стать оплотом защиты населения от киберпреступности. Основным выводом проведённого исследования является то, что такое совершенствование образования позволит повысить общую цифровую грамотность населения, уровень доверия общества к государству, а в частности к органам правопорядка. Обеспечит быстрый, всесторонней поиск вредоносных сайтов, в виду чего их количество, как и негативный эффект от таковых, понизится, что приведёт к снижению киберпреступности в России.

Ключевые слова:

Кибербезопасность, киберпреступления, национальная безопасность, школьное образование, цифровая трансформация образования, проверка подлинности сайта, международные отношения, сеть Интернет, профилактика, обучение

В процессе культурного и социального развития общество неуклонно стремилось к информатизации. Из поколения в поколение совершенствовались способы передачи и хранения информации. И в настоящее время весь поток данных проходит через глобальную сеть Интернет, с появлением которой началась история киберпреступлений.

Несмотря на относительно недавнее появление, данная тематика активно рассматривалась такими исследователями как: А.Г. Асмолов, Ю.Н. Бирюкова, А.Г. Ковалева, И.В. Челышева.

В настоящее время научно-технический прогресс настолько тесно связан с человеком, что большая часть населения проводит значительную часть своего времени в электронной среде: хранит в ней свои денежные средства, активы, персональные данные и другую важную информацию о себе. Тесная связь тематики с жизнью современного и будущего человека обуславливает её общественную значимость.

«Интернет проник уже во все сферы нашей жизни, и, по большому счету, он должен все же подчиняться даже не просто законам, формальным юридическим правилам, но и моральным законам общества, в котором мы живем. Иначе это общество будет разрушаться изнутри» - сказал Президент России Владимир Путин в марте 2021 года на встрече с участниками общероссийской акции взаимопомощи «Мы вместе» [17].

Для оценки роста интеграции цифровой среды в нашу жизнь рассмотрим статистические данные. На январь 2022 года общая численность населения России составляла 145,9 млн. человек, из них 75,2 % проживают в городах, а 24,8 % в сельской местности [22]. Как нам известно, в городах частота взаимодействия человека и технологий значительно выше, чем в сельской местности.

Согласно отчёту о состоянии цифровой сферы GlobalDigital 2022 по состоянию на январь 2022 года в России насчитывается 129,8 млн интернет-пользователей. Интернетом пользуются от 89% от общей численности населения [32]. По данным Kepios, за 2021 год количество интернет-пользователей в России увеличилось на 5,8 млн (+4,7%).

Среднестатистический житель России проводит в интернете примерно 7 часов 5 минут в сутки и 46,7% этого времени - на мобильных устройствах. Пользователями социальных сетей стали 106 млн человек или 72,7% от общей численности населения. За 2021 год количество пользователей социальных сетей в России увеличилось на 7 млн (+7,1%) [22].

Эти цифры дают понимание объёмов внедрения и роста цифровых технологий, но чтобы понять, что люди на самом деле делают в интернете, нам нужно глубже погрузиться в данные. Главная причина использования интернета у российских интернет-пользователей - поиск информации. 84,3% пользователей из России в возрасте от 16 до 64 лет выходят в онлайн именно с такой целью. На втором месте - общение с родственниками и друзьями (66,4%), а за новостями в сети следят 66,1% жителей России [15].

Можно сделать вывод о том, что процесс наполнения нашей жизни информационными технологиями неуклонно растёт. Технологии во многом упрощают жизнь современному человеку: не нужно постоянно носить тяжелый кошелёк, достаточно пользоваться бесконтактной оплатой или идти в организацию и заполнять целые горы документов, повторяя одни и те же данные о себе по нескольку раз, а просто зарегистрироваться на соответствующем сайте и составить их дистанционно.

Учащаются случаи, когда в результате работы с информационной средой наши данные получаются и используются киберпреступниками и мошенниками в корыстных целях. Кроме того, современные технологии используются для преступлений, которые посягают на половую неприкосновенность несовершеннолетних, психическое здоровье граждан, посягают на имущественное положение государства, юридических и физически лиц, могут носить террористический или экстремистский характер, что в свою очередь подрывает национальную безопасность страны в целом.

По статистике количество киберпреступлений в России выросло в 11 раз за 5 лет, до свыше 510,4 тыс. случаев, то есть на 94,6% [28].

С начала 2022 года сумма ущерба от IT-преступлений в России составила 65 млрд рублей (сообщает ТАСС со ссылкой на слова главы МВД России Владимира Колокольцева), что превысило данные 2021 года на 20% [27]. Не стоит оставлять без внимания и тот факт, что большинство преступлений совершается со стороны зарубежных стран. Учитывая современную геополитическую ситуацию, защита населения от иностранных киберпреступников, как никогда актуальна и в тоже время значительно усложнилась.

Стремительная интеграция технологий в повседневность, повышает угрозу кибератак мошенников, которые все чаще, для совершения своих действий используют подростков. К примеру, за определённое вознаграждение предлагают распространять вредоносные программы.

Рост киберпреступности является сегодня актуальной проблемой, т.к. каждое четвертое преступление в России происходит с помощью информационных технологий или в киберпространстве. А правоохранительные органы не успевают справляться с растущими объемами таких преступлений. Только III квартале 2022 г. хакеры взломали 22,3 млн российских акаунтов [19]. 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 – все это виды угроз государству, а следовательно, и угроза национальной безопасности [22].

Киберпреступления являются одной из самых серьезных угроз для современных людей и организаций. По мере развития технологий кибербезопасности злоумышленники только усложняют свои атаки, используя новые данные. Поэтому каждой отрасли нужны эксперты по кибербезопасности, чтобы остановить хакеров на их пути и защитить конфиденциальные данные компании. Благодаря такому высокому спросу ожидается, что число рабочих мест для специалистов по кибербезопасности вырастет на 33% с 2020 по 2030 год [24].

На Международном конгрессе по кибербезопасности в Москве (2019 г) Владимир Путин озвучил список мер по киберзащите страны, которые намерено принять правительство [14]. В список вошли международное сотрудничество, создание системы обмена информацией о кибератаках, использование отечественного ПО и подготовка квалифицированных кадров.

Традиционные подходы к расследованию преступлений не позволяют в полной мере противостоять этому качественно новому виду угроз. Необходимым условием успешной работы в этом направлении является понимание сотрудниками правоохранительных органов специфики функционирования киберсферы, ее трансграничного характера, умение работать в информационной среде, взаимодействовать с представителями IT-компаний и другими специалистами, знать, как и где искать доказательства, как их фиксировать. И конечно грамотно построить диалог с участниками уголовного процесса, допросить свидетелей, подозреваемых и обвиняемых в совершении таких преступлений.

Андрей Ковалёв, начальник главного управления по противодействию киберпреступности МВД Беларуси, отметил, что киберпреступность развивается. И правоохранительные органы не имеют права отстать: «Преступники стали более грамотными, они идут в ногу со временем, используют определенные гаджеты, технологии. Мы как минимум должны им соответствовать. А в идеале должны быть на шаг впереди и предвидеть то или иное преступное деяние, которое может совершиться с учетом той же геополитической ситуации и всего происходящего в мире» [10].

В соответствии с президентским Указом от 30 сентября 2022 г. № 688 создано Управление МВД РФ по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК) [3].

Среди основных задач управления: предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе министерства. Подразделение будет также осуществлять анализ данных, содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия преступности. Управление сотрудничает с ФСБ, госорганами, учреждениями финансово-кредитной системы, организациями информационно-коммуникационной сферы, иными участниками информационного обмена, включая агрегаторов больших данных.

На официальном интернет-ресурсе СБ РФ после заседания, посвященного вопросам нейтрализации внутренних угроз национальной безопасности (27 января 2022 года), отмечается: «Представители научной общественности высказались за необходимость

включения в школьные образовательные программы и в образовательный процесс федеральных и национальных университетов страны элементов информационной безопасности».

В настоящее время данной проблеме уделяется большое внимание, но еще не сформировались общенаучные подходы, и публикации носят скорее исследовательский характер. Часть процессов подчиняется общим законам развития организаций, данный аспект рассмотрен в научных трудах и исследованиях достаточно полно [5;18]. Представители высшей школы, и, в частности, Высшей школы экономики, изучают эти процессы более глубоко. А.Ю. Уваров считает, что цифровая трансформация является естественной составляющей текущих процессов развития образования, и выделяет три группы сценариев [26]. Для каждого сценария важную роль играет внедрение цифровых технологий, однако технологические решения при этом могут абсолютно различаться. Анализ современных тенденций, показал, что цифровая трансформация образования, определяется доминантой дальнейшего развития [25]. М.А. Селиванова в своих исследованиях основное внимание уделяет роли обучающих цифровых платформ. В связи с наличием запроса в обществе на упорядочение подходов к цифровой трансформации образовательных организаций разрабатываются методические рекомендации, в которых собраны нормативно-законодательные документы, систематизированы основные определения и требования, приведены модели, технологии и инструменты [31].

Реформируемая под процессы цифровизации общества и экономики система образования должна создать условия для содействия гражданам в формировании цифровых компетенций, для достижения массовой цифровой грамотности и возможности персонализации образовательной траектории в форме индивидуальной образовательной траектории формирования компетенций [11].

Для решения этих задач осуществляется ряд проектов, и к 2024 г. ожидается создание такой системы образования, которая могла бы выявлять талантливую молодежь, особенно в ИТ-сфере, обеспечивать подготовку высококвалифицированных кадров, востребованных в условиях Индустрии 4.0, а также масштабную реализацию программ переподготовки и повышения квалификации в более узких профессиональных областях с учетом достижений цифровизации. В рамках данного направления важным является и то, что построение любой цифровой инфраструктуры очень тесно взаимосвязано с деятельностью, основанной на инновационном подходе [11].

В сложившихся условиях предусмотренные процессы цифровой трансформации отрасли выступают необходимым фундаментом для решения поставленных перед системой науки и образования задач.

Процессы цифровой трорансформации широко представлены в стратегии цифровой трансформации отрасли науки и высшего образования, принятой распоряжением Правительства РФ «Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования» от 21 декабря 2021 г. № 3759-р.

Согласно стратегии, школьники должны изучать основы кибербезопасности на уроках ОБЖ и технологии. По согласованию с Министерство просвещения почти половина учебной программы предмета ОБЖ будет посвящена изучению основ безопасности в интернете. На уроках технологии школьников будут учить навыкам безопасного использования различных цифровых сервисов. Минцифры считает, что занятия по

информатике для этого не предназначены, так как на них преподаются информационные технологии и принципы их применения [19].

С 2022 года ученикам 8-11 классов будут доступны в удаленном режиме специальные двухгодичные курсы программирования. Дополнительное бесплатное профессиональное обучение программированию поможет школьникам определиться с будущей профессией и сформировать навыки, востребованные в цифровой экономике [29].

Во многих ВУЗах страны была введена новая дисциплина, которая так и называется «Кибербезопасность». Эти новшества должны помочь нашим гражданам справиться с угрозами, возникающими при работе с электронной средой.

Самые обыденные проблемы, с которыми может столкнуться пользователь электронной среды, это фальшивые сайты в ресурсе Интернет: ложные магазины, берущие оплату, но не доставляющие товар; страницы, необоснованно требующие паспортные данные, данные банковских карт и многие другие. Далеко не каждый человек сможет отличить сайт оригинала от сайта мошенников без наличия определённых знаний в этой сфере, а страницы мошенников появляются в интернете прямо как гидра – закрывается один сайт, на его месте появляется два новых.

Конечно, существуют определённые алгоритмы действий и специальные люди, которые занимаются поиском и закрытием вредоносных электронных страниц. В основном это сайты-клоны. Сайты-клоны — это способ мошенничества с помощью фишинга. Фишинг (fishing – рыбная ловля) — это противоправное действие, с помощью которого мошенники пытаются заставить лицо сообщить им конфиденциальную информацию.

Проверка сайта на подлинность — это скорее творческий процесс, нежели точный план действий. Ни один из предложенных способов не может стопроцентно гарантировать подлинность ресурса, но, если использовать их в совокупности, проверка сайта на мошенничество будет успешнее. Приведем примерный порядок действий:

1. **Проверить домен**: мошенники регистрируют домены, которые максимально схожи с оригинальным ресурсом: могут вставить символ или цифру между словами (kino0poisk.ru), добавляют дополнительную букву или заменяют букву (muz**i**ika.ru), меняют доменную зону (muzika.site).

2. **Проверить, есть ли SSL:**в начале адресной строки можно увидеть один из 2-х видов протоколов: http:// или https://. Если вы видите http://, это говорит о том, что на сайте не установлен SSL-сертификат, который проверяет подлинность сайта и защищает данные пользователя от перехвата мошенниками**.** Однако даже если вы видите https://, не стоит расслабляться. Есть некоторые виды SSL, которые нетрудно получить. Мошенники понимают, что даже рядовые пользователи нередко знают об опасности http-протокола, да и браузеры стали предупреждать юзеров большими сообщениями или красными пометками. Мошенники тратят деньги и время на установку хотя бы простого сертификата. Поэтому пользователю нужно нажать на значок замочка рядом с URL: здесь будет информация о сертификате и об удостоверяющем центре (УЦ), который его выдал.

3. **Проверить данные о регистрации домена**: перейти в сервис Whois, ввести доменное имя и нажать **«**Проверить» (как давно домен используется, зарегистрирован на физическое или юридическое лицо и соответствует ли это типу сайта. Например, на сайте указан крупный бренд, а в Whois указано физическое лицо).

4. **Посмотреть контент на сайте**: создавать полноценный веб-ресурс с множеством страниц мошенникам невыгодно. Они создают всего лишь пару страниц с товарами, корзину и макет формы для оплаты.

5. **Обратить внимание на платёжные системы**: мошенники не используют платёжные системы, которые работают с банковскими картами. Чаще всего для оплаты они предлагают воспользоваться QIWI-кошельком. Поэтому, если при оплате товара или услуги вас отправляют только на QIWI-кошелек, стоит задуматься.

6. Обратиться к сервисам для проверки безопасности веб-ресурсов. Например, такой сервис есть у Google у сервиса VirusTotal. Современные антивирусы способны отслеживать фишинговые сайты. Например, с 2019 года такая функция есть у антивируса Avast.

7. **Посмотреть, как выглядел сайт некоторое время назад, проверить снапшоты**. Снапшот — это снимок сайта. То есть, система периодически обходит ресурсы, сохраняет их внешний вид и грузит эти данные в большой архив. На сайте web.archive.org вы можете ввести URL-адрес и посмотреть, как он выглядел, например месяц назад. На сайты мошенников часто жалуются, поэтому им постоянно приходится переезжать. Если веб-ресурс существует недолго или на нём постоянно меняется контент (то один интернет-магазин, то другой), возможно, этот сайт недобросовестный.

Если вы стали жертвой мошенника или смогли распознать его до кражи, помогите другим пользователям не попасться на удочку. Для этого свяжитесь с владельцами настоящего веб-ресурса и сообщите им о сайте-клоне. Они со своей стороны смогут обратиться к хостинг-провайдеру и потребовать удалить вредоносный сайт. Также о нарушении вы можете сообщить поисковым системам. Google и Яндекс создали формы для жалоб на сайты.

С 1 декабря 2021 года в России начали блокировать мошеннические сайты по инициативе Банка России во внесудебном порядке в течение нескольких дней, согласно федеральному закону от 1 июля 2021 года N 250-ФЗ. Раньше эта процедура могла занимать месяцы. По новому механизму Банк России будет передавать списки мошеннических интернет-ресурсов в Генеральную прокуратуру, у которой есть полномочия направлять предписания об их внесудебной блокировке в Роскомнадзор. Такой алгоритм взаимодействия позволит в сжатые сроки ограничивать доступ граждан к сайтам финансовых пирамид и другим мошенническим площадкам, которые действуют в Интернете под видом финансовых организаций. Принятый закон также дает регулятору право обращаться в суд с заявлением об ограничении доступа к ресурсам, распространяющим вредоносное программное обеспечение.

«Новый закон позволит сократить финансовые потери наших граждан от действий злоумышленников. Сейчас преступники успевают обмануть много людей, прежде чем доступ к мошенническому сайту будет закрыт. Такая практика, в частности, характерна для финансовых пирамид. Принятие закона позволит изменить ситуацию», — отметил заместитель Председателя Банка России Герман Зубарев [16].

Онлайн-мошенники особенно активизировались во время пандемии COVID-19, так как граждане предпочитали получать услуги и сервисы в основном в дистанционном формате. За I квартал 2021 года было выявлено 124 нелегальных форекс-дилера, 85 финансовых пирамид и 144 нелегальных кредитора. В целом порядка 45% нелегальных участников финансового рынка и финансовых пирамид действуют именно в Интернете

[16].

Но, как бы то ни было, полностью победить этот недуг в настоящее время не предоставляется возможным. А что, если количество людей, способных определить подлинность интернет-страниц и знающих алгоритмы действий для завершения работы мошеннических сайтов, возрастёт по численности до целой страны? Когда школьники и студенты ещё во время обучения смогут находить фальшивые и вредоносные сайты и помогать уполномоченным органам в их ликвидации.

Проведя исследование данной темы предлагаем, совершенствовать программу обучения школьников таким образом, чтобы в ней обучали навыкам отличия безопасных и не безопасных интернет-страниц, а программу обучения студентов так, чтобы они могли отличать дополнительно запрещённый это сайт или нет и соответствует ли он правилам работы в той сфере, в которой студент получает образование. Например, представители юридических специальностей могут определить разрешена ли продажа товара, расположенного на сайте в России. А также, в процессе такого обучения, предоставить образовательной организации возможность для обучающихся сообщать о таких сайтах специальному работнику и стимулировать обучающихся к этому.

Для достижения работоспособности данного предложения необходимо достичь совершенствования материально-технической базы в образовательных организациях, которая будет соответствовать условиям новых стандартов обучения.

Необходимо отметить, что программа по комплектации учреждений новыми технологиями уже проводится. Но во многих образовательных организациях нашей страны оснащённость современными техническими устройствами, используемыми в процессе обучения, оставляет желать лучшего. Кроме того, учебные заведения, которые имеют большое количество современных технических средств, зачастую не используют их в процессе обучения.

Для достижения цели необходимы дополнения к учебным пособиям или их полная переработка. Школьники и студенты должны иметь хорошо проработанную, актуальную информацию для процесса своего обучения. А так же необходима подготовка педагогических кадров, способных грамотно объяснять обучающимся все аспекты действий по обнаружению и ликвидации вредоносных программ и мошеннических сайтов. Кроме того, в обязанности педагога, преподающего соответствующий предмет, должны входить обязанности по приёму и проверки информации от обучающихся о вредоносных сайтах и программах. В результате чего, анализируя полученную информацию, они смогут предоставлять её в правоохранительные органы для дальнейшей проверки. Что в свою очередь так же требует налаживание взаимодействия органов правопорядка и сферы образования в данном направлении.

Дополняя нововведения, стоит так же отметить необходимость в стимулировании обучающихся. Должна присутствовать система способов и методов поощрения граждан в зависимости от проделанной работы.

Таким образом, население сможет более предметно овладеть базовыми навыками безопасной работы с интернет-ресурсами, повысить свою киберграмотность, помочь обществу и государству, выработать чувство гражданского долга.

В среднем, каждый день мы просматриваем более двух новых страницы в информационных ресурсах всё чаще попадая на противоправные. Их рост напрямую угрожает национальной безопасности страны, которая уже проводит ряд действенных

контрмер по борьбе с киберпреступностью. Но при налаживании указанного ранее способа взаимодействия между образовательными организациями и системой Министерства внутренних дел, наша страна сможет повысить свою защищённость от киберпреступлений, скорость выявления и раскрытия преступлений, связанных с информационными системами. Что позволит ещё раз доказать всему миру высокий уровень образованности и защищённости нашей страны.

Библиография

1. А. Михайлова. Проблемы кибербезопасности в России и пути их решения / ГАРАНТ.РУ / Информационно-правовой портал / Аналитическая статья / URL: https://www.garant.ru/article/520694/
2. Бирюкова Ю.В. Проблемы, возникающие при расследовании хищений, совершенных с использованием компьютерных и телекоммуникационных технологий, и пути их решения. Вестник Московского университета МВД России. 2021;(4):137-142
3. В структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий / Официальный сайт МВД РФ / URL: https://мвд.рф/news/item/32844180/
4. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.
5. Герасимов Б.Н. Реинжиниринг процессов организации / Б.Н. Герасимов. — Москва: Вуз. учеб., 2017. —256 с.
6. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.
7. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.
8. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. — М.: ГЛТ, 2017. — 536 с.
9. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.
10. Ковалев О. Г. Современная киберпреступность: криминологический и уголовно-правовой анализ [Электронный ресурс] / О. Г. Ковалев // Борьба с преступностью: теория и практика: тезисы докладов IX Международной научно-практической конференции (Могилев, 23 апреля 2021 года) / Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь»; редкол.: Ю. П. Шкаплеров (отв. ред.) [и др.]. – Могилев: Могилев. институт МВД, 2021. – 1 электрон. опт. диск (CD-R). – С. 48–52.
11. Константинова Д.С. Цифровые компетенции как основа трансформации профессионального образования / Д.С. Константинова, М.М. Кудаева. — DOI: 10.18334/et.7.11.111073 // Экономика труда. — 2020. —Т. 7, № 11. — С. 1055–1072.
12. Лагутин П.Д. Киберпреступность как актуальная угроза обществу / П. Д. Лагутин, Т. А. Миханова. — Текст: непосредственный // Молодой ученый. — 2018. — № 42 (228). — С. 108-109. — URL: https://moluch.ru/archive/228/53137/ (дата обращения: 26.02.2023).

13. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
14. Пленарное заседание Международного конгресса по кибербезопасности / Раздел: Новости, выступления и стенограммы / Текстовая версия. URL:http://www.kremlin.ru/events/president/news/57957
15. Популярные соцсети: что изменилось в 2023 году / Статья/ Редакция сайта GreekBrains / URL: https://gb.ru/blog/populyarnye-sotsseti/
16. Процедура блокировки мошеннических сайтов значительно ускорится / Банк России / новости / URL: https://cbr.ru/press/event/?id=11007
17. Путин заявил о способности интернета разрушить общество изнутри / А. Дружинин /пресс-служба президента РФ / ТАСС / https://tass-ru.cdn.ampproject.org/v/s/tass.ru/obschestvo/10834539
18. Реинжиниринг производственных процессов / Д.С. Бурцев, Е.С. Гаврилюк, А.Г. Изотова, Н.А. Литвинова. — Санкт-Петербург: Ун-т ИТМО, 2021. — 50 с.
19. Российские школьники будут изучать основы кибербезопасности на уроках ОБЖ и технологии / Информационная служба Хабра / Учебный процесс в IT /Законодательство в IT / URL: https://habr.com/ru/news/t/576394/
20. Россия обогнала США, став самой взламываемой страной в мире / А. Патракова / ИТ-маркетплейс Market CNews / URL:https://cnews.ru/link/n558815
21. Семененко В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.
22. Статистика интернета соцсетей в России на 2022 год. URL: https://www.web-canape.ru/business/internet-v-rossii-v-2022-godu-samye-vazhnye-cifry-i-statistika/
23. «Стратегия цифровой трансформации отрасли науки и высшего образования» (утв. Минобрнауки России) / Юридическая информационная система «Легалакт-законы, кодексы и нормативно-правовые акты Российской Федерации» / URL: https://legalacts.ru/doc/strategija-tsifrovoi-transformatsii-otrasli-nauki-i-vysshego-obrazovanija-utv/
24. Топ-10 вариантов онлайн степени кибербезопасности на 2022 год / URL:https://translated.turbopages.org/proxy_u/en-ru.ru.f61e63bc-6400d279-96503224-74722d776562/https/hackr.io/blog/online-cyber-security-degree
25. Трудности и перспективы цифровой трансформации образования / под ред. А.Ю. Уварова, И.Д. Фрумина. — Москва: Изд. дом Высш. шк. экономики, 2019. — 343 с.
26. Уваров А.Ю. Цифровая трансформация и сценарии развития общего образования / А.Ю. Уваров. — Москва: Изд-во НИУ ВШЭ, 2020. — 108 с.
27. Ущерб от IT-преступлений в России с начала года вырос на 20% / URL: https://www.kommersant.ru/doc/5620873
28. Число киберпреступлений в России. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России
29. Школьники смогут бесплатно учиться программированию с 2022 года /В. Крайнов / ТАСС / URL: https://tass.ru/obschestvo/12214121
30. Цифровая трансформация в образовании: проблемы и перспективы развития: сб. материалов Межрегион. науч.-практ. конф. / под ред. М.А. Селивановой, К.А. Ротобыльского, А.Н. Гончаровой [и др.]. — Липецк: Ин-т развития образования, 2021. — 162 с.
31. Цифровая трансформация образования: метод. рекомендации / сост. Г.А. Сумина, Е.Ю. Новикова. — Саратов: Изд-во СОИРО, 2021. — 26 с.430 Bulletin of Baikal State

University, 2022, vol. 32, no. 2, pp. 423–431
32. Global Digital 2022: ежегодный отчёт об интернете и социальных сетях — главные цифры / Исследования / URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Политика кибербезопасности современного образования».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам реализации в России политики кибербезопасности в сфере современного образования. Автором рассматривается актуальность указанной проблемы, приводятся система эмпирических и теоретических аргументов, подчеркивающий значимость имеющейся проблематики, предлагаются некоторые оригинальные идеи по поводу того, в каком направлении должна идти политика кибербезопасности современного образования. В качестве предмета исследования выступили эмпирические данные, мнения ученых, положения правовых актов и т.п.

Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о перспективных направлениях политики кибербезопасности в сфере современного образования. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из эмпирических данных.
Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства (прежде всего, положений правовых актов РФ). Например, следующий вывод автора: «Процессы цифровой трорансформации широко представлены в стратегии цифровой трансформации отрасли науки и высшего образования, принятой распоряжением Правительства РФ «Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования» от 21 декабря 2021 г. № 3759-р».
Также важными в контексте цели исследования стали эмпирические методы исследования, которые позволили на основании различных данных и статистики показать актуальность и значимость тематики, разрешить иные важные моменты по работе. Так, автор пишет: «По статистике количество киберпреступлений в России выросло в 11 раз за 5 лет, до свыше 510,4 тыс. случаев, то есть на 94,6% [28]. С начала 2022 года сумма ущерба от IT-преступлений в России составила 65 млрд рублей (сообщает ТАСС со ссылкой на слова главы МВД России Владимира Колокольцева), что превысило данные 2021 года на 20% [27]. Не стоит оставлять без внимания и тот факт,

что большинство преступлений совершается со стороны зарубежных стран. Учитывая современную геополитическую ситуацию, защита населения от иностранных киберпреступников, как никогда актуальна и в тоже время значительно усложнилась».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема политики кибербезопасности в сфере современного образования сложна и неоднозначна. С одной стороны, использование онлайн ресурсов необходимо для образования и просвещения детей. С другой стороны, сеть «Интернет» может негативным образом влиять на детское психическое и физиологическое здоровье. Автор прав в том, что «Учащаются случаи, когда в результате работы с информационной средой наши данные получаются и используются киберпреступниками и мошенниками в корыстных целях. Кроме того, современные технологии используются для преступлений, которые посягают на половую неприкосновенность несовершеннолетних, психическое здоровье граждан, посягают на имущественное положение государства, юридических и физически лиц, могут носить террористический или экстремистский характер, что в свою очередь подрывает национальную безопасность страны в целом». С практической стороны следует признать, что необходимы конкретные предложения по поводу разрешения поставленной проблемы.
Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.
Научная новизна предложенной статьи не вызывает сомнений. Она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«Проведя исследование данной темы, предлагаем совершенствовать программу обучения школьников таким образом, чтобы в ней обучали навыкам отличия безопасных и не безопасных интернет-страниц, а программу обучения студентов так, чтобы они могли отличать дополнительно запрещённый это сайт или нет и соответствует ли он правилам работы в той сфере, в которой студент получает образование. Например, представители юридических специальностей могут определить разрешена ли продажа товара, расположенного на сайте в России. А также, в процессе такого обучения, предоставить образовательной организации возможность для обучающихся сообщать о таких сайтах специальному работнику и стимулировать обучающихся к этому».
Также можно выделить и иной важный вывод:
«Для достижения цели необходимы дополнения к учебным пособиям или их полная переработка. Школьники и студенты должны иметь хорошо проработанную, актуальную информацию для процесса своего обучения. А так же необходима подготовка педагогических кадров, способных грамотно объяснять обучающимся все аспекты действий по обнаружению и ликвидации вредоносных программ и мошеннических сайтов. Кроме того, в обязанности педагога, преподающего соответствующий предмет, должны входить обязанности по приёму и проверки информации от обучающихся о вредоносных сайтах и программах. В результате чего, анализируя полученную информацию, они смогут предоставлять её в правоохранительные органы для дальнейшей проверки. Что в свою очередь так же требует налаживание взаимодействия органов правопорядка и сферы образования в данном направлении».
Приведенные выводы может быть актуален и полезен для правотворческой деятельности.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.
Тематика статьи соответствует специализации журнала «Право и политика», так как она посвящена правовым проблемам, связанным с правовой политикой в области образования.
Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.
Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Бирюкова Ю.В., Гафнер В.В., Герасимов Б.Н., Громов Ю.Ю., Ефимова Л.Л., Запечников С.В. и другие). Хотело бы отметить использование автором большого количества эмпирических данных и статистики, что позволило придать исследованию правоприменительную направленность. Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к направлениям совершенствования политики в области образования в целях достижения кибербезопасности.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»