**Proхnchev** **Gennadi Borisovich** is a Candidate of Physics and Mathematics, Associate Professor; Deputy Dean of Faculty of Sociology of Lomonosov Moscow State University, Moscow, Russia, e-mail: pronchev@rambler.ru

**Goncharova Inna Vladimirovna** is a Candidate of Pedagogical Sciences, Associate Professor; Associate Professor of the Department of Social Technologies at Faculty of Sociology of Lomonosov Moscow State University, Moscow, Russia, e-mail: ig73@inbox.ru

**Mikhailov Aleksander Petrovich** is a Doctor of Physics and Mathematics, Professor, Chief Researcher at Keldysh Institute of Applied Mathematics of the Russian Academy of Sciences. Moscow, Russia. E-mail: apmikhailov@yandex.ru

**Lyubimov Aleksei Pavlovich** is a Doctor of Law, Professor, Deputy Chief Scientific Secretary of the Presidium of the Russian Academy of Sciences, Head of the Centre for International Law of Diplomatic Academy of the Ministry of Foreign Affairs of Russia, Moscow, Russia, e-mail: gosduma624@yandex.ru

**О проблемах информационной безопасности учебного процесса в период пандемии коронавируса** **COVID-19**

**Аннотация**: Актуальность исследуемой проблемы обусловлена тем, что в период пандемии коронавирусной инфекции COVID-19 и временным переводом учебного процесса в дистанционный формат, участники учебного процесса столкнулись с новыми информационными угрозами в виртуальных образовательных средах. Цель статьи заключается в анализе информационных угроз для участников учебного процесса в виртуальных образовательных средах Рунета и предложения мер для их купирования. Теоретическим подходом к исследованию данной проблемы является структурный и сравнительный анализ. Эмпирическим методом исследованию данной проблемы является Интернет-исследование о вовлеченности пользователей Рунета в изучаемые проблемы и выявления наиболее популярного для них контента. В работе анализируются социально-правовые аспекты использования дистанционной формы обучения в Российской Федерации. Приведена классификация возникающих информационных угроз. Обсуждаются механизмы устранения возникающих угроз. Несмотря на то, что Россия прилагает значительные усилия на законодательном уровне с целью предотвращения вредоносного информационного воздействия на участников учебного процесса, тем не менее, ряд особенностей виртуальных социальных сред не позволяет в полной мере их реализовать. Полученные результаты могут представлять интерес для специалистов, занимающихся проблемами современного образования, информационного противоборства, информационной безопасности виртуальных социальных сред.

**Ключевые слова**: виртуальные образовательные среды, Интернет, COVID-19, информационные угрозы

**1. Introduction**

Пандемия коронавируса COVID-19 принесла для современного общества необходимость решения большого количества новых задач (Pronchev & Sushko, 2021). Одной из таких задач является переход учебных заведений на дистанционный формат обучения (Sushko & Pronchev, 2021). По прошествии времени с начала пандемии такой переход уже не воспринимается как временное неудобство (Cherepanova, 2020). Очевидно, что с окончанием пандемии дистанционные формы обучения будут продолжать активно использовать параллельно с традиционными обучающими формами. Как показали наши исследования, и до начала пандемии коронавируса COVID-19 интерес к дистанционной форме обучения был достаточно велик (Pronchev, Goncharova, Pronchev, & Krichever, 2019). Как следствие этого, дистанционные формы обучения необходимо развивать с методической и дидактической точек зрения.

В настоящее время дистанционное обучение рассматривается как процесс взаимодействия между различными участниками для передачи и получения нового знания или решения научно-технической проблемы, отличительной чертой которого является интеграция, перенос научных знаний и традиционных обучающих форм в цифровое пространство (Monakhov & Pronchev, 2020). Получение знаний в настоящее время невозможно без использования современных информационно-коммуникационных технологий и созданных на их базе виртуальных социальных сред (Pronchev, Monakhov, Proncheva, Mikhailov, 2018), так же, как и обучение конкретной дисциплине невозможно без привлечения соответствующих информационно-коммуникационных ресурсов.

Необходимо отметить, что помимо несомненных преимуществ, которые открывает использование виртуальных социальных сред, они же несут и серьезные риски. В предыдущих наших работах обсуждались проблемы безопасности, связанные с работой в виртуальных социальных средах (Pronchev, Mikhailov, Lyubimov, Solovyev, 2020; Goncharova, Pronchev, Rodionova, Krichever, 2022). Runet users' attitude to the outrageous content in virtual social environments. *Academic Journal of Interdisciplinary Studies*, 11(1):258–268. ), а также появившиеся новые риски, связанные с пандемией COVID-19 (Pronchev, Shisharina, Proncheva, 2021).

Целью данной работы является анализ рисков для информационной безопасности учебного процесса, возникающих в период пандемии коронавируса COVID-19 в России.

**2. Literature review**

Педагогический энциклопедический словарь дает следующее определение: «Дистанционное обучение – технология целенаправленного и методически организованного руководства учебно-познавательной деятельностью учащихся (независимо от уровня получаемого ими образования), проживающих на расстоянии от образовательного центра. Дистанционное обучение осуществляется с помощью средств и методов педагогического общения преподавателя и обучаемого при минимальном количестве обязательных занятий. По методам организации учебного процесса Дистанционное обучение близко к заочной форме обучения, а по насыщенности и интенсивности учебного процесса – к очной форме» (Dictionary, 2002).

К преимуществам дистанционных форм обучения относят гибкий график, отсутствие территориальной привязки, к недостаткам, в первую очередь, нет методически выверенной технологии построения учебной деятельности на основе дистанционного обучения, возникают вопросы информационной безопасности всех участников процесса и др. (Pronchev, Goncharova, Pronchev, & Krichever, 2019).

Понятие информатизации в образовании тесно связано с вопросами глобализации образования, направленного на сближение национальных традиций и технологий обучения, на выработку единых образовательных стандартов, что становится возможным, благодаря быстро развивающимся информационным технологиям (Goncharova, Pronchev, Tretyakova, 2017).

Возникает острая необходимость регламента основных обучающих принципов. Использование современных образовательных платформ на базе виртуальных социальных сред позволяет разграничить такие понятия как дистанционное и заочное обучение. Дистанционное обучение предполагает проведение онлайн-занятий в режиме реального времени с применением интерактивных обучающих методик и материалов (Goncharova, Pronchev, Tretyakova, 2017). В этом смысле, можно говорить о технологичности образовательного процесса. Важным аспектом является выполнение требования доступности. Нельзя допускать возможности появления образовательного неравенства (Pronchev, Monakhov, Proncheva, Mikhailov, 2018). У всех обучающихся и преподавателей должны быть одинаковые, равные возможности доступа к устройствам и приложениям: образовательным платформам, ресурсам или иным технологиям взаимодействия учителя и ученика. Помимо этого, образовательный процесс носит массовый характер. Используемые устройства должны быть хорошо известны широкому кругу пользователей, а коммуникационные приложения, образовательные платформы или ресурсы должны быть ориентированы на широкий круг пользователей с соблюдением возрастных особенностей. Дистанционное обучение должно быть построено с учетом норм пребывания за компьютером пользователей разных возрастных категорий, в особенности детей школьного возраста. Особое внимание должно быть уделено правильной организации рабочего пространства. Таким образом, необходимо соблюдение здоровьесберегающего принципа. Важно, чтобы при переходе в онлайн-формат основные дидактические принципы оставались неизменными: научность, доступность, целенаправленность, систематичность и последовательность, наглядность, связь обучения. (Goncharova & Pronchev, 2020).

Серьезной проблемой при переходе на электронное обучение с применением дистанционных образовательных технологий является информационная безопасность.

Информационные риски, связанные с работой в виртуальных социальных средах, которые обсуждались в наших работах ранее (Pronchev, Mikhailov, Lyubimov, Solovyev, 2020), присутствуют и в образовательных виртуальных средах (Pronchev & Goncharov, 2017). Во-первых, это касается непосредственно учебно-методической информации, во-вторых, персональной конфиденциальной информации об участниках учебно-воспитательного процесса. Информация может быть похищена, испорчена, изменена, удалена.

Следует отметить, что возможные последствия несанкционированных преподавателем действий против первого и второго типа информации сильно различаются. Если в первом случае в качестве последствий могут быть лишь временные затруднения в организации учебно-воспитательного процесса и оценки реальных знаний обучаемых, то во втором случае возникают проблемы с безопасностью людей (Pronchev & Goncharov, 2017).

По проблемам безопасности второго типа информации в виртуальных социальных средах ранее нами была дана классификация возможных угроз для конфиденциальной информации, выявлены потенциальные злоумышленники, предложена информационно-логическая модель защиты конфиденциальной информации в виртуальных социальных средах (Korablev, Lontsov & Pronchev, 2010).

Информационная безопасность может быть классифицирована не только как система мер, направленная на защиту информационного пространства от возможных попыток хищения учебно-методической и персональной информации, хакерских атак с целью внесения изменений в конфигурацию системы, но и как защита образовательного процесса от распространения запрещенной информации, например, порнографии, пропаганда насилия, вовлечения участников образовательного процесса в криминальные структуры и т.д.

Информационные угрозы могут иметь намеренный и ненамеренный характер. Ко вторым относятся технические неисправности аппаратуры, аварийные ситуации, сбой в работе систем связи. К намеренным угрозам относятся и хулиганские действия со стороны третьих лиц, например, широкую огласку получили факты несанкционированного подключения порнохакеров во время учебных видеоконференций (Runev, 2020). Несанкционированный доступ может быть осуществлен хакерами напрямую, через непосредственный доступ к серверу или компьютеру с дальнейшим копированием информации на посторонний носитель. Также могут быть использованы специальные программы, осуществляющие взлом, копирование, перехват информации и другие технические средства в зависимости от целей злоумышленников.

На государственном уровне меры по защите информации в Российской Федерации регулируются законодательной базой, опирающейся на Конституцию РФ (Constitution, 1993) и ряд базовых подзаконных актах. К последним следует отнести: Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности» (FZ, 2010), Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (FZ, 2006a), Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (FZ, 2006b), «Стратегию национальной безопасности Российской Федерации», утвержденную Указом Президента Российской Федерации от 31 декабря 2015 года № 683 (Decree, 2015) и «Доктрину информационной безопасности Российской Федерации», утвержденную Указом Президента Российской Федерации от 9 сентября 2000 года № 646 (Decree, 2016) и другие правовые акты. Все другие последующие акты были нацелены на конкретизацию и реализацию данных документов (Lyubimov, & Shchitov, 2017).

Помимо указанного, необходимо соблюдение авторских прав и соблюдение прав на базы данных.

В настоящее время довольно успешно применяются технические инструменты для обеспечения целости информационной системы, к которым относятся специализированные программные продукты, например, DLP-системы и SIEM-системы, стоимость которых достаточно высока (Kulagina, 2016). Широко используются антивирусные программы, эффективность которых оценивается по-разному.

В комплексе мер по защите информации административные меры учебного заведения прописывают внутренние правила и порядок работы с информацией, сюда же можно отнести и физические меры, предусматривающие пропускную систему различной степени допуска в компьютерные помещения.

Социально-этические средства обеспечения информационной безопасности – комплекс мер, который в настоящее время только формируется. Социально – этические нормы должны рассматриваться в контексте профилактики девиантного поведения в виртуальных социальных средах (Pronchev, 2020). Впервые в истории человечества не старшее поколение учит молодежь, а наоборот, молодое поколение, владеющее новыми техническими знаниями. Виртуальное пространство- пространство молодых людей, которые, не всегда готовы нести ответственность за свои действия, более того, создается чувство безнаказанности, приводящее к различного рода девиациям (Pronchev, 2020).

Виртуальные социальные среды Рунета являются самым крупным источником информации для большей части российской молодежи, которая одновременно является самым активным пользователем Интернета. По результатам исследования «Социальный портрет современного российского студента» (Osipova, Sinykov, Elishev, Kanevsky & Trofimov, 2018), было установлено, что «из всех видов СМИ, подавляющее большинство студентов (93,9%) отдают предпочтение различным интернет-СМИ (95,5% - студентов-бакалавров младших курсов, 93,8% - бакалавров старших курсов, 91,1% - студентов-магистров) и всего лишь 4% - телевидению (2,7% - студентов-бакалавров младших курсов, 4,8% - бакалавров старших курсов, 5,6% - студентов-магистров). Слушать радио и обращаться к периодическим печатным изданиям предпочитает совсем незначительное число опрошенных. В большинстве случаев Интернет используется для общения (91,9% ответов), поиска необходимой информации (90,7% ответов), развлечений (73,3% ответов), учебы (67,4% ответов), работы (43,1% ответов), игр (11,5% ответов) (Osipova, Sinykov, Elishev, Kanevsky & Trofimov, 2018).

Очевидно, что необходима серьезная работа в поле создания кодекса этических правил в сфере использования информационно-коммуникационных технологий, направленный на цифровое нравственное воспитание молодежи, учитывающий международные традиции. В качестве примера можно привести кодекс этики для информационного общества Юнеско (Ethics, 2011)

Цифровое воспитание должно базироваться на общепринятом определении воспитания как “деятельности, направленной на развитие личности, создание условий для самоопределения и социализации обучающегося на основе социокультурных, духовно-нравственных ценностей и принятых в обществе правил и норм поведения в интересах человека, семьи, общества и государства” (FZ, 2012).

В целом поведение высоконравственной личности в цифровом пространстве должно отвечать таким качествам как уважительное отношение к людям и себе, информационным и технологическим процессам, аппаратному решению, чувства долга и ответственности, оказание товарищеской помощи (Goncharova & Pronchev, 2015; Monakhov, Goncharova, Pronchev, 2018). Information systems on the basis of modern information and communication technologies as a tool for the formation of leadership qualities. In *Leadership for the Future Sustainable Development of Business and Education*, Springer Proceedings in Business and Economics, pages 521–529).

Приобщение молодежи к проблеме информационной безопасности реализует основные принципы нравственного воспитания и является решением ряда задач:

* Во-первых, это установление координации цифрового воспитательного процесса с учебной и научной деятельностью, которые все более имеют цифровой направленный характер и переносятся в виртуальное пространство.
* Во-вторых, это создание микроклимата для полноценного вхождения молодежи в социальное виртуальное пространство, обеспечение условий для становления молодых людей как нравственной личности с четкими принципами цифрового поведения, осознающего свою ответственность за будущее развитие виртуального пространства и технологий.
* В-третьих, это развитие профессиональной цифровой компетенции молодых людей в контексте общего цифрового мировоззрения.
* В-четвертых, это обеспечение мероприятий по поддержанию инициатив творческой и талантливой молодежи, реализация индивидуального подхода в воспитательной работе.

Цифровое воспитание, так же, как и нравственное воспитание, формируется в целостной системе образовательного процесса. Учащиеся «не создают понятий, образцов, ценностей и норм общественной морали, а присваивают их в процессе учебной деятельности. Но в процессе ее выполнения... осуществляют мыслительные действия, адекватные тем, посредством которых исторически вырабатывались эти продукты духовной жизни» (Davydov, 1986). Такое понимание находит свое отражение в технических условиях, научных статьях, образовательных стандартах, затрагивающих вопросы информационной безопасности.

**3. Methodological Framework**

Объектом данного исследования являются информационные угрозы для участников учебного процесса.

Целью исследования является анализ информационных угроз для участников учебного процесса в виртуальных образовательных средах и предложения мер для их купирования.

В связи с пандемией коронавирусной инфекции COVID-19 и переходом образовательного процесса в России на электронное обучение с активным применением дистанционных форм, проблема информационной безопасности участников учебного процесса получила дополнительную актуальность.

Задачи исследования:

1. анализ информационных угроз для участников учебного процесса в виртуальных образовательных средах Рунета;
2. анализ российских нормативных документов, регламентирующих информационную безопасность в виртуальных образовательных средах;
3. проведение эмпирического Интернет-исследования о вовлеченности пользователей Рунета в изучаемые проблемы и выявления наиболее популярного для них контента;
4. предложения по купированию угроз, существующих в виртуальных образовательных средах Рунета.

Ведущим теоретическим подходом к исследованию данной проблемы является структурный и сравнительный анализ. Эмпирическим методом исследованию данной проблемы является Интернет-исследование о вовлеченности пользователей в изучаемые проблемы и выявления наиболее популярного для них контента.

In this work, the Internet study conducted by the authors in November 01, 2021 was used as the source of empirical data. Процедура проведения исследования была аналогична той, что использовалась нами в работе (Pronchev, Goncharova & Proncheva, 2020)

In the Internet study, the hypothesis about there being a stable and significant statistical relation between the activity of users in the Internet communities associated with a particular topic (descriptors) and the level of significance of the selected topic for them (indicators) (Petrov & Pronchev, 2017; Pronchev, Goncharova, Pronchev & Krichever, 2019).

The Popsters analytical service (Online: https://popsters.ru. Available November 01, 2021) was used as a toolkit. Various metrics of the Popsters resource were employed (see Table 1).

**Table 1:**The Popsters Resource Metrics

|  |  |
| --- | --- |
| **Name of the metric** | **Description** |
| **ER**(abbr. Engagement Rate) | users' engagement rate of the content published (**posts**); |
|  | ERpost | users' engagement rate of a particular posts**ERpost = (likes + reposts + comments [+ dislikes for YouTube]) / quantity of followers** |
|  | ERday | total users' engagement rate for all posts published within a day |
|  | ERview | engagement rate of a particular post calculated as the number of views (for VKontakte, YouTube, Coub, and Flickr)**ERview = (likes + reposts + comments [+ dislikes for YouTube]) / quantity of views of the published item** |
|  | average ERpost | the arithmetic average of ERpost for all published items for the period under analysis |
|  | average REview | the arithmetic average of ERview of all the posts |
|  | average ERday | the arithmetic average of ERday for the entire period under analysis |
| **LR**(abbr. Love Rate) | love rate (**"likes" only**)**LR = (The total of likes) / quantity of followers/quantity of published items for the period under analysis** |
| **TR**(abbr. Talk Rate) | talk rate (**comments only**)**TR = (The total of comments) / quantity of followers/quantity of published items for the period under analysis** |

**Source: (Pronchev, Goncharova & Proncheva, 2020)**

**4. Results and Discussions**

Научно-обоснованной концепции соединения цифрового воспитания и обучения, в том числе и дистанционного обучения, к сожалению, на сегодня нет. Для реализации такого масштабного проекта, на наш взгляд, необходимо изучение отношения участников виртуальных социальных сред к этической стороне информационной безопасности в компьютерной сети. В частности, изучение мнения пользователей социальных сетей.

Исследование проводилось 01 ноября 2021 года.

По запросу «Информационная безопасность» в социальной сети «Вконтакте» зарегистрировано 4688 сообществ, с максимальным числом подписчиков 195064 в группе «Хакер/хакер.ru-взом, безопасность».

По типу контента условно можно поделить на несколько групп: профессиональное сообщество программистов и специалистов по информационной безопасности, политическая информационная безопасность, образовательные услуги разной направленности, благотворительные фонды.

**Figure 1.** Распределение Интернет-сообществ по типу контента (%).

**Source: the authors**

Для дальнейшего анализа использовался ресурс Popsters (popsters.ru). Исследовалась активность пользователей на заданную тематику в период 29.09.2021- 30.10.2021.

При анализе профессионального сообщества рассматривались все группы. В таблице 1 представлены группы с количеством подписчиков более 10 тысяч. Основной контент- карикатуры на профессиональную тему, способы защиты информации и ее взлома.

**Table 1: Интернет-сообщества с количеством подписчиков более 10 тысяч**

**Source: the authors**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Сообщества****(транслитерация)** | **Смысловой перевод** | **Количество подписчиков** | **Количество просмотров** | **Вовлеченность в процентах** |
| Хакеры | Этичный хакинг с Михаилом Тарасовымhttps://vk.com/public44038255 |  | 12508 | 61561 | 0,2332 |
| PSH-WORLD | Информационная Безопасностьhttps://vk.com/public3457574 |  | 21668 | 1223 | 0,1638 |
| Служба поддержки - Вход.руhttps://vk.com/public42119847 |  | 46186 | 22406 | 0,0204 |
| Хакер / xakep.ru — взлом, безопасность и защитаhttps://vk.com/public10933209 |  | 195065 | 99723 | 0,0078 |
| overpublic1https://vk.com/public79759696 |  | 133272 | 821554 | 0,2106 |
| Разработка iOS, Android, WEB App. Namasam IThttps://vk.com/public53773933 |  | 11681 | 0 | 0 |
| RTM Group | ИТ-эксперты и юристы | Аудит ИБhttps://vk.com/public11189040 |  | 12235 | 1228 | 0,0041 |
| GreyTeam | Хакерыhttps://vk.com/public169106523 |  | 11286 | 359390 | 0,6155 |
| Информационная безопасностьhttps://vk.com/public69741303 |  | 10013 | 2282 | 0,3196 |
| The Codebyhttps://vk.com/public75857525 |  | 10005 | 162476 | 0,3587 |

На основе активности пользователей в сообществах можно судить о различных рейтингах, такие, как лайки, комментарии, репосты, коэффициенты вовлеченности.

По коэффициенту вовлеченности ERpost, который рассчитывается как частное от суммы лайков, репостов и комментариев на количество подписчиков пользователей в публикуемый контент можно выделить пост сообщества «Хакеры| Этичный хакинг с Михаилом Тарасовым» – Хакинг на примерах (2,99%) и пост Сообщества «GreyTeam| Хакеры» (2,029%). Первый пост – это представление книги A.A. Yaroshenko “Hacking by examples. Vulnerabilities, hacking, protection” (Yaroshenko, 2021), второй пост – карикатура под лозуногом «Хватит создавать трояны и ратники».

В целом, короткий текст в профессиональных сообществах доминирует и составляет до 80 % от общего контента с преобладанием коротких постов- карикатур, в которых комический эффект различных действий нарушения информационной безопасности обсуждается на профессиональном сленге (73%).

Подписчики активно участвовали в обсуждении постов, которые условно можно разделить на категории, представленные на Figure 2.

**Figure 2.** Распределение комментариев по тематике (%).

**Source: the authors**

В комментариях к постам участники пишут о важности работы, возникающих проблемах, делятся опытом, при этом общение ведется на сленге, понятном для программистов и специалистов по информационной безопасности.

**Figure 3.** Содержание комментариев (%).

**Source: the authors**

В теме обсуждения вовлечения несовершеннолетних можно выделить пост «Да что вы знаете об анонимности» сообщества «The Codeby» о создании фиктивного приложения «Дия». Это - украинская программа, которая позволяла школьникам покупать алкоголь и сигареты, подделывая возраст в электронном паспорте. Оплату за приложение разработчик получал на свою карту, что было опрометчиво. Как и ожидалось, он был быстро пойман. Разработчиком оказался 21-летний парень из Украины. Теперь ему грозит до 6 лет тюрьмы (Codeby, 2021).

В комментариях участники сообщества осуждают подобные действия, однако, сомневаются, что властям удалось найти реального разработчика (Codeby, 2021).

Таким образом, можно с уверенностью говорить о том, что профессиональное сообщество категорически осуждает все формы взлома, противоправных действий, хакинга и объединяется вокруг идеи информационной безопасности.

При анализе образовательных сообществ рассматривались все группы, в таблице 2 представлены группы с количеством подписчиков от 5 тысяч.

**Table 2: Образовательные Интернет-сообщества с количеством подписчиков более 5 тысяч**

**Source: the authors**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Сообщества****(транслитерация)** | **Смысловой перевод** | **Количество подписчиков** | **Количество публикаций** | **Количество просмотров** | **Вовлеченность в процентах** |
| Life-Hack / Жизнь-Взломhttps://vk.com/public163703907 |  | 24319 | 115 | 670205 | 1,7620 |
| Академия энерго - информационной безопасности.https://vk.com/public115516032 |  | 23147 | 16 | 1390 | 4,1440 |
| OTUS. Онлайн-образованиеhttps://vk.com/public145052891 |  | 10457 | 133 | 79848 | 0,5636 |
| PSH-WORLD | Информационная Безопасностьhttps://vk.com/public3457574 |  | 21666 | 1 | 405 | 6,6667 |
| Информационная безопасностьhttps://vk.com/public69741303 |  | 10014 | 1 | 1,811 | 2,3744 |
| Ростовский колледж связи и информатики (РКСИ)https://vk.com/public75021 |  | 7025 | 40 | 90,303 | 1,0240 |
| Кибердружина Волгоградская областьhttps://vk.com/public138547391 |  | 5,862 | 3 | 646 | 3,9854 |
| Pentestithttps://vk.com/public40086034 |  | 5,716 | 1 | 2,356 | 0,5518 |

*По количеству просмотров 10 наиболее популярных тематик (количество раз):*

1. Борьба с поддельными QR кодами (48730).
2. Создание фейковой страницы с порнографическим контентом (37601).
3. Смена технических средств для обеспечения функций оперативно-розыскных мероприятий (27332).
4. Хакер украл медный кабель (27116).
5. Samsung извинилась за российское ПО на смартфонах жителей Великобритании (26533).
6. Android-телефоны постоянно следят за своими пользователями (25231).
7. Американка взломала систему летной школы, чтобы отомстить бывшему (23085).
8. Microsoft признала, что ряд пользователей Windows может столкнуться с проблемами сетевой печати (19267).
9. Шпионские планы инженера-атомщика раскрыл агент ФБР под прикрытием (14396)
10. Новый вредонос AbstractEmu рутит мобильные устройства на Android (14010).

*Первые 10 постов по количеству лайков (понравилось, количество раз):*

1. Взлом любой системы при помощи USB (124).
2. Отмена учебных занятий в связи с пандемией (107).
3. 10 поисковых систем используемых хакерами (106).
4. Взлом Windows 10 (105).
5. Создание сканера портов на Python (89).
6. Проникновение в маршрутизаторы с помощью Routersploit (84).
7. Поиск и удаление вредоносных программ из Linux (79).
8. Основы Linux для начинающих хакеров (78).
9. 16 сервисов помогающих бесплатно получить иформацию (73).
10. Взлом паролей беспроводных сетей (68).

*Первые 10 постов по, которые репостили (количество раз):*

1. Взлом любой системы при помощи USB (177).
2. 10 поисковых систем используемых хакерами (137).
3. Отмена учебных занятий в связи с пандемией (131).
4. Проникновение в маршрутизаторы с помощью Routersploit (123).
5. Взлом Windows 10 (118).
6. Взлом паролей беспроводных сетей (105).
7. Основы Linux для начинающих хакеров (102).
8. Создание сканера портов на Python (96).
9. Сбор информации из разных источников (81).
10. 16 сервисов помогающих бесплатно получить иформацию (80).

*Первые 10 постов по вовлеченности (в %):*

1. Отмена учебных занятий в связи с пандемией (3,388%).
2. Взлом любой системы при помощи USB (1,250%).
3. Завтрак с директором (1,011%).
4. 10 поисковых систем используемых хакерами (0,999%).
5. Взлом Windows 10 (0,921%).
6. Проникновение в маршрутизаторы с помощью Routersploit (0,851%).
7. Декада пожилого человека, День памяти участников Великой Отечественной войны (0,811%).
8. Создание сканера портов на Python (0,761%).
9. Взлом паролей беспроводных сетей (0,740%).
10. Основы Linux для начинающих хакеров (0,740%).

*Первые 10 постов по количеству оставленных комментариев с тональностью (количество раз):*

1. В России придумали метод борьбы с поддельными QR-кодами. Разработчики из новосибирской команды Pro Control создали некопируемый QR-код с двухфакторной системой проверки (22).

Тональность комментариев негативная. Технология не является совершенной, легко поддается взлому, нет аппаратов для считывания подобных кодов. Разработка подобной технологии больше похожа на осваивание выделенных бюджетных денег. Такая технология только усложняет жизнь обычных граждан.

1. Воронежский хакер украл медный кабель на 10 млн рублей (20).

Тональность комментариев позитивная. Участники осуждают действия хакера, однако, удивлены из чего может быть сделан «медный кабель» за 10 млн. рублей.

1. Глава Росфинмониторинга: террористы получают финансирование через валюту в компьютерных играх (16).

Тональность комментариев положительная: участники вполне допускают мысль о финансовой поддержке террористов через компьютерные игры, однако, есть мнения о государственном контроле игровой индустрии с целью дополнительного налогообложения.

1. Android-телефоны постоянно следят за своими пользователям (16).

Тональность комментариев положительная. Участники обеспокоены и осуждают сбор персональных данных со сматрфонов.

1. Samsung извинилась за российское ПО на смартфонах жителей Великобритании (11).

Тональность комментариев нейтральная.

1. Смена технических средств для обеспечения функций оперативно-розыскных мероприятий (10).

Тональность комментариев негативная: осваивание бюджетных средств.

1. Взлом паролей беспроводных сетей (7).

Тональность комментариев нейтральная: профессиональное обсуждение поста.

1. Роскомнадзор собирается оштрафовать Google на 22 млрд. рублей (7).

Тональность комментариев негативная. Участники не поддерживают решение Роскомнадзора.

1. Microsoft признала, что ряд пользователей Windows может столкнуться с проблемами сетевой печати (6).

Тональность комментариев негативная.

1. Предполагаемому хакеру Twitter предъявлено обвинение в краже криптовалюты на сумму 784 тысячи долларов через обмен SIM-картами (5).

Тональность комментариев нейтральная. Участники удивляются как один человек смог такое сделать.

Обобщая полученные эмпирические данные, можно констатировать:

* Посты носят краткий информационный характер, наблюдается короткая длина текста.
* Наблюдается пересечение постов по всем категориям рейтинга.
* Наблюдается существенный разрыв между количеством просмотров и остальными категориями рейтинга.
* Несмотря на то, что этот блок сообществ был отнесен к образовательному блоку, пользователи отмечали посты по обшей теме информационной безопасности, не связанной с образованием.
* Обратная связь может быть прослежена по коэффициенту вовлеченности в пост.
* Количество комментариев немногочисленное, но тем не менее, оно позволяет проанализировать мнение пользователей, уловить тональность сообщения.
* Участники негативно оценивают действия хакеров, радеют за разумные решения в области информационной безопасности, выступают за разумное расходование бюджетных средств, негативно относятся к сбору персональных данных без согласия.

**5. Conclusion and Recommendations**

Пандемия коронавируса COVID-19, в связи с переходом обучения в виртуальные социальные среды, принесла новые информационные угрозы для участников учебного процесса.

Российское общество негативно оценивает действия злоумыщленников в виртуальных социальных средах.

Несмотря на то, что государственная власть в России прилагает значительные усилия на законодательном уровне с целью предотвращения вредоносного информационного воздействия на участников виртуального учебного процесса в Рунете, ряд особенностей виртуальных социальных сред не позволяет в полной мере их реализовать. Тем не менее, государству необходимо и дальше продолжать работу в этом направлении.

Необходима серьезная работа по созданию кодекса этических правил в сфере использования виртуальных образовательных сред, направленный на цифровое нравственное воспитание молодежи.

Как механизм борьбы с информационными угрозами необходимо повышать уровень образования пользователей виртуальных образовательных сред (как обучаемых, так и преподавателей) (Pronchev, Proncheva & Goncharova, 2019).

**Acknowledgements**

This research was supported by the Russian Science Foundation (project no. 20-11-20059, Keldysh Institute of Applied Mathematics RAS).

**References**

Cherepanova, Yu. (2020). Between the first and second: online education in the wake of a pandemic. *Forbes Education*, 08.10.2020. URL: https://education.forbes.ru/authors/online-education-vs-covid. (Retrieved October 31, 2021).

Codeby. (2021). What do you know about anonymity? The Codeby. VK.COM, 27.10.2021. URL: https://vk.com/wall-75857525\_9939. (Retrieved October 30, 2021).

Constitution. (1993). Russian Constitution. Adopted by popular vote on December 12, 1993 with changes approved in the all-Russian vote on July 1, 2020. *President of Russia*. URL: http://kremlin.ru/acts/constitution. (Retrieved October 30, 2021).

Davydov, V.V. (1986). Problems of developing learning: The experience of theoretical and experimental psychological research. Moscow: Pedagogy, 240 p.

Decree. (2015). Decree of the President of the Russian Federation of December 31, 2015 No. 683. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/40391. (Retrieved October 30, 2021).

Decree. (2016). Decree of the President of the Russian Federation of December 05, 2016 No. 646. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/41460. (Retrieved October 30, 2021).

Dictionary. (2002). Pedagogical Encyclopedic Dictionary. Ch. ed. B.M. Bim-Bad. Moscow: Big Russian Encyclopedia, 527 p.

Ethics. (2011). Code of Ethics for the Information Society proposed by the Intergovernmental Council of the Information for All Programme (IFAP). *UNESDOC*. URL: https://unesdoc.unesco.org/ark:/48223/pf0000212696. (Retrieved October 30, 2021).

FZ. (2006a). Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technologies and Information Protection”. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/24157. (Retrieved October 30, 2021).

FZ. (2006b). Federal Law No. 152-FZ of July 27, 2006 “On Personal Data”. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/24154. (Retrieved October 30, 2021).

FZ. (2010). Federal Law No. 390-FZ of December 28, 2010 “On security”. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/32417. (Retrieved October 30, 2021).

FZ. (2012). Federal Law No. 273-FZ of December 29, 2012 “On Education in the Russian Federation”. *President of Russia*. URL: http://www.kremlin.ru/acts/bank/36698 (Retrieved October 30, 2021).

Goncharova, I.V., Pronchev, G.B. (2015). Moral education of young people in the context of helping people with disabilities. *Education and Upbringing*, **2**, 66–69.

Goncharova, I.V., Pronchev, G.B. (2020). Regulation of the basic principles of distance learning in the context of the covid-19 pandemic. COVID-19 as a factor of reflection of social inequality. International Scientific Conference. Collection of materials. Moscow: MAX Press, 61–63. URL: https://www.socio.msu.ru/documents/20210111\_sbornik.pdf. (Retrieved October 30, 2021).

Goncharova, I.V., Pronchev, G.B., Rodionova, M.E., Krichever, E.I. (2022). Runet users' attitude to the outrageous content in virtual social environments. *Academic Journal of Interdisciplinary Studies*, **11(1)**, 258–268. https://doi.org/10.36941/ajis-2022-0023.

Goncharova, I.V., Pronchev, G.B., Tretyakova, I.V. (2017). Innovations in the field of mathematical and information training of sociology students in the context of globalization processes. *Education and Law*, **8**, 241-253.

Korablev, M.N., Lontsov, V.V., Pronchev, G.B. (2010). Protection of confidential information in Internet social networks. *Sociology*, **4**, 33-45.

Kulagina, T. (2016). How information is protected in Russia. *RUNET*, 01.09.2016. URL: https://runet.news/articles/7960. (Retrieved October 30, 2021).

Lyubimov, A.P., & Shchitov, A.N. (2017). RGAIS-the leader in the profiles of training in the field of protection of intellectual property rights. *Representative power-XXI century*, 4, 18-20.

Monakhov, D.N., Goncharova, I.V., Pronchev, G.B. (2018). Information systems on the basis of modern information and communication technologies as a tool for the formation of leadership qualities. In *Leadership for the Future Sustainable Development of Business and Education*, Springer Proceedings in Business and Economics, 521–529. https://doi.org/10.1007/978-3-319-74216-8\_52.

Monakhov, D.N., Pronchev, G.B. (2020). From a digit to the digital society. *Political Science Issues*, **10(3)**, 277–284. https://doi.org/10.35775/PSI.2020.42.3.002.

Osipova, N.G., Sinykov, A.V., Elishev, S.O., Kanevsky, P.S., Trofimov, S.V. (2018). A social portrait of the modern Russian student. By results of a research at sociological faculty of Lomonosov Moscow State University. Moscow: FGBUN ISPI of RAS. 56 p.

Petrov, A.P., Pronchev, G.B. (2017). Collection of empirical data for the model of dynamics of interest in a political event. In Mathematical Modeling of Social Processes, 19, 75-79. Moscow: Keldysh Institute of Applied Mathematics RAS. URL: http://keldysh.ru/social/2016. (Retrieved October 30, 2021).

Pronchev, G.B. (2020). On the features of virtual social environments contributing to social deviations. *Education and Law*, **3**, 200–208. https://doi.org/10.24411/2076-1503-2020-10334

Pronchev, G.B., Goncharov, I.V. (2017). Security of modern electronic educational environments. *Distance and Virtual learning*, **3**, 26-30.

Pronchev, G.B., Goncharova, I.V., Pronchev, K.G., Krichever, E.I. (2019). Russians' attitude to distance learning: a Runet survey. *International Journal of Learning, Teaching and Educational Research*, **18(11)**, 370–384. https://doi.org/10.26803/ijlter.18.11.22.

Pronchev, G.B., Goncharova, I.V., Proncheva, N.G. (2020). The range of communication topics of the visually impaired in the internet communities. *Humanities and Social Sciences Reviews*. **8(4)**, 301–314. https://doi.org/10.18510/hssr.2020.8431.

Pronchev, G.B., Mikhailov, A.P., Lyubimov, A.P., Solovyev, A.A. (2020). Particularities of the internet-based virtual social environments within the context of information warfare. *EurAsian Journal of BioSciences*, **14**, 3731–3739.

Pronchev, G.B., Monakhov, D.N., Proncheva, N.G., Mikhailov, A.P. (2018). Contemporary virtual social environments as a factor of social inequality emergence. *Astra Salvensis*, **6**, 207–216.

Pronchev, G.B., Proncheva, N.G., Goncharova, I.V. (2019). Modern management of media environment: negative effects for the society of today. *Journal of Environmental Treatment Techniques*, **7(4)**, 836–840.

Pronchev, G.B., Shisharina, E.V., Proncheva, N.G. (2021). Cyber threats for modern Russia in the context of the coronavirus pandemic. *Political Science Issues*, **11(1)**, 26–34. https://doi.org/10.35775/PSI.2021.48.1.003.

Pronchev, G.B., Sushko, V.A. (2021). Influence of the coronavirus pandemic on social processes in Russia. *AD ALTA*, **11(1)**, 310–315. https://doi.org/10.33543/1101.

Runev, I. (2020). In Moscow, students were shown porn in a remote lesson. *KP.RU*, 16.04.2020. URL: https://www.kp.ru/online/news/3838914. (Retrieved October 31, 2021).

Sushko, V.A., Pronchev, G.B. (2021). Online learning in the context of pandemic in Russia. *Revista Romaneasca pentru Educatie Multidimensionala*, **13(2)**, 1–17. https://doi.org/10.18662/rrem/13.2/407.

Yaroshenko, A.A. (2021). Hacking by examples. Vulnerabilities, hacking, protection. St. Petersburg: Science and Technology, 320 p.