

## Кибербезопасность в цифровой учебной среде


### **Александр Сергеевич Олейник**

студент

Национальный исследовательский ядерный университет «МИФИ»

Москва, Россия

sasha010698z@yandex.ru

 0000-0002-8021-3799


### **Алексей Николаевич Шилов**

студент

Дальневосточный федеральный университет

Владивосток, Россия

alexshow245@gmail.com

 0000-0000-0000-0000


### **Данил Анатольевич Светличный**

студент

Национальный исследовательский Московский государственный строительный университет

Москва, Россия

danilsve4@gmail.com

 0000-0001-6559-4549


### **Роман Александрович Макаров**

студент

Национальный исследовательский Московский государственный строительный университет

Москва, Россия

roma.makaro2001@yandex.ru

 0000-0001-6550-8751


### **Анастасия Александровна Мартазаева**

студент

Санкт-Петербургский государственный экономический университет

Санкт-Петербург, Россия


martazaeva.nasty@mail.ru

 0000-0000-0000-0000

Поступила в редакцию 18.04.2022

Принята 09.05.2022

Опубликована 20.06.2022

 10.25726/ 7435-3301-1451-c

### **Аннотация**

Люди живут и действуют в цифровом пространстве (ЦП). Дети рождаются, растут, учатся и будут работать с гаджетами, которые подключены к сетям и становятся естественной средой. Их жизнь находится под влиянием и воздействием ЦП со старыми и новыми опасностями, зависит все больше от когнитивных факторов, интерфейса, контента, моделей поведения) и может характеризоваться с позиций безопасности, эффективности комфортности (в частности здоровья), то есть находится в поле деятельности эргономистов. Возникают новые проблемы, вызванные жизнью и деятельностью в ЦБ,

соответствующими факторами влияния, способами их избегания и соответствующими новыми средствами и инструментами. Соответственно требующие решения проблемы развития и внедрения информационно-коммуникационных технологий (ИКТ) в образовании, на чем акцентируется внимание как на международном, так и национальном уровнях. Однако следует учитывать, что «под влиянием новых информационных технологий происходят процессы трансформации общественного развития столь фундаментальные и глобальные, что, кроме положительного влияния, закономерно несут с собой серьезные проблемы, угрозы и риски в случае недооценки новых факторов и условий». Как отмечалось в материалах Международных Форумов в Давосе (2018-2019 гг), особую остроту приобретает проблема кибербезопасности (КБ), которое касается практически всех сфер жизни и деятельности человека, особенно в условиях полной информатизации образования. Из-за кибератак человечество терпит убытки более чем на 400 млрд. США в год.

#### **Ключевые слова**

кибербезопасность, вуз, институт, защита.

#### **Введение**

Ключевые проблемы информатизации образования в России определены в Национальном докладе 2020 г.: «О состоянии и перспективах развития образования в России»: формирование и широкое внедрение единого образовательного информационного пространства России и обеспечение надлежащего научного сопровождения этих процессов; развертывание и усовершенствование необходимых элементов инфраструктуры региональных информационных и телекоммуникационных сетей, взаимосвязанных как между собой, так и с глобальной сетью Интернет; низкий уровень ИКТ и информатических компетентностей населения; фактическая несформированность целостной национальной политики применения ИКТ в образовании, недостаточная правовая база.

Новые вызовы времени и новые направления развития общества – Общество 4.0, Образование 4.0 (Озерова, 2017), проникновения новых технологий во все сферы жизни, «гибридная» война – требуют понять ключевые проблемы и вопросы безопасности образовательного процесса в цифровом пространстве, в частности безопасность всех непосредственных участников, организаторов образования, государства, а также безопасности содержания обучения

С охватом информатизацией всех сфер жизни человека значение кибербезопасности вышло на уровень компетентности по вопросам безопасности жизнедеятельности человека и даже превысило его.

По данным 2017 Norton Cyber Security Insights Report, 978 млн. граждан стран G-20 в 2017 г. стали жертвами киберпреступности. С целью предотвращения этого явления принимаются национальные и региональные программы (Соколова, 2013), создаются международные центры (Соколова, 2017), принимаются программы совместного действия (Соколова, 2018), утверждаются стандарты (Vasbieva, 2018).

По оценкам мировых экспертов в 2016 г., мировые расходы на кибербезопасность превышали 70 млрд. долл. США в год с ежегодным ростом на 10-15%. В частности, по данным экспертов Gartner, Inc. рост таких расходов в 2018 г. ожидался в размере до 93 млрд. долл. США (Антонова, 2012).

#### **Материалы и методы исследования**

В России актуальна подготовка специалистов по кибербезопасности проводится в 182 вузах. Как правило, будущие специалисты и в России, и в других странах получают теоретические знания и практические навыки по программированию, разработке и управлению базами данных, формированию моделей защиты информации и политик безопасности, технической и криптографической защите информации, построению защищенных цифровых TCP/IP сетей и обслуживанию сертификатов открытых ключей, тестирования систем на проникновение, администрированию защищенных информационных и коммуникационных систем, проведению их мониторинга и аудита и тому подобное (Ломов, 1012).

Однако через 5 лет после принятия стандарта ISO (Vasbieva, 2018) начало существенно меняться видение проблемы кибербезопасности, поскольку человек все больше перестает быть лишь субъектом киберпреступлений, превращаясь в объект сам по себе, а не только его финансовые и экономические интересы и возможности (Озерова, 2017). Так, по данным аналитической компании RAND Corporation, структура кибер-рисков изменилась в последние годы (Пряжников, 2018).

Все больше аналитиков обращают внимание на то, что основные причины инцидентов в интернет-ресурсах в 2017 г. связаны с действием человеческого фактора, массовым изломом IoT-устройств и облачных сервисов. Особенно эта проблема обостряется с усилением цифрового гуманистического характера образования (Соколова, 2013), ростом роли социальных сетей в жизни человека в целом и образовании в частности (Соколова, 2017), а также пониманием человечества необходимости перехода к образованию в течение жизни (Соколова, 2018).

За три последних года на поприще реформирования образования во многих экономически развитых странах произошла разработка ключевых документов, которые стали ориентирами для педагогов, среди которых разработана и представлена в странах ЕС Рамка цифровой компетентности для граждан 2.0-2.1 (Digital Competence Framework for Citizens 2.0-2.1).

В Федеральном Законе Об образовании информационно-коммуникационная компетентность определена одной из ключевых компетенций. Вопрос кибербезопасности является важными составляющими этой компетентности и отражают общие подходы, сформулированные в Рамках цифровой компетентности для граждан ЕС.

Вопросы кибербезопасности остро стоят с тех пор, как компьютерная техника перестала быть лишь прерогативой крупных научных центров. С появлением и распространением локальных и глобальных сетей изменилось понимание кибербезопасности, соответствующих трендов, проблем и задач. Рассмотрим их с учетом трансформации образования в направлении цифрового образования, образования 4.0.

### **Результаты и обсуждение**

Современная жизнь все больше и больше строится вокруг цифровых сетей, а социальные медиа становятся новым социальной средой (Пряжников, 2018). Вмешательство в эти сети создает реальную угрозу безопасности в области образования и страны в целом.

В качестве узла могут выступать «агенты» сети - люди (создатели ресурса и его контента, администраторы ресурса, постоянные или случайные пользователи), технические (терминальные станции, компьютеры, подключенные к сети гаджеты, коммуникаторы) и информационные (базы данных, базы знаний, управляющие системы и т. п.) средства.

Все агенты в зависимости от их природы имеют присущий им интерфейс и виды связи с другими агентами. Однако следует заметить, что одновременно с развитием технологий построения сетей, их усложнением, использованием искусственного интеллекта, появлением облачных и туманных технологий, ростом мощности баз данных (БД) и баз знаний (БЗ) сеть перестала быть просто посредником между пользователями (средство коммуникации).

Поскольку информация в глобальной сети существует вне очерченного пространства и времени, сама сеть становится активным агентом воздействия на человека (Ведута, 2020), сохраняя, прежде всего, общедоступными большие объемы данных (Антонова, 2012). Любой пользователь может войти в сеть (легально или нелегально) и получить доступ к необходимым узлам (при использовании облачных средств конкретные узлы обычному пользователю могут быть неизвестными), изменяя также их контент (например, Wikiобъект) по разрешенным правилам.

Однако информация в БД и БЗ по разрешенными правилами может быть изменена или внесена с целью искажения представление пользователей о данных, которые они ищут. Определенные пользователи могут использовать это для влияния на широкую или целевую аудиторию, «искажая» нужные узлы (технической или информационной природы) или воздействуя на них средствами социальной инженерии (если узел – это человек) (Гаджиева, 2016).

Поскольку сеть является системой связанных узлов, то поврежденный («искаженный») узел может повлиять уже сам по себе на вторичные узлы. Кроме того, искаженная информация начинает существовать в Сети даже независимо от человека («агрессора»), который ее ввел.

Любой рассмотрение проблем кибербезопасности как самостоятельного фактора СЛТС является ограниченным и лишь частично эффективным, поскольку не учитывает изменения, происходящие с агентами СЛТС не только во времени, но и в пространстве, которое расширяется с развитием технологий от локального до глобального. Соответствующие изменения происходят и в отношении учебной среды (УС).

УС является одним из краеугольных камней образования. Существует много различных определений и классификаций УС. На наш взгляд, «учебная среда-это искусственно построенная система, структура и составляющие которой способствуют достижению целей учебно-воспитательного процесса» (Соколова, 2013). «Целесообразно говорить о УС как об окружающей среде в отношении интеллектуальных составляющих педагогической системы - составляющих, которые наделены естественным или искусственным интеллектом».

УС оказывает многофакторное влияние на субъектов учебного процесса, изменяясь как во времени, так и в пространстве. Причем это справедливо как для традиционного УС, так и для синтетического. Отмечается, что «... учебная среда в содержательном плане возникает всегда как динамический процесс формирования сети отношений в субъекте обучения, в который (не всегда осознанно) избирательно вовлекаются самые разные элементы внешнего и/или внутреннего окружения...» (Васильева, 2017), причем такой динамический процесс является характерным для любого УС, но в иммерсивном и виртуальном УС приобретает еще большую остроту из-за более глубокого погружения ученика в процесс обучения.

Разные авторы различают естественные и искусственные, предметные и информационно-динамические, адаптивные и другие УС, используя различные критерии их типологизации, например, по стилю взаимодействия внутри среды, по характеру отношения к социальному опыту и его передаче, по степени творческой активности, по характеру взаимодействия с внешней средой (Соколова, 2018). Однако ко времени наибольшее внимание привлекает цифровое или киберпространство из-за обострения проблемы безопасности человека в нем, прежде всего, молодого человека, формирование которого только происходит как в личностном, так и компетентностном измерении.

Проблемы, что кажутся локальными, могут нарастать и быстро распространяться, создавая угрозы и системные риски. Уязвимость в киберпространстве является реальной, серьезной и она быстро разрастается. Объекты инфраструктуры особой важности, разведка, коммуникации, командование и контроль, торговля и финансовые операции, логистика, ликвидация последствий и готовности к чрезвычайным ситуациям полностью зависят от ИТ-систем, объединенных в сети (Дубровский, 2021).

Нарушения кибербезопасности, кража данных и интеллектуальной собственности не знают границ. Они влияют на все - от личной информации до государственных тайн.

Киберпространство можно рассматривать как триаду, в которую входят:

- 1) информация, в своем цифровом представлении: статическая (файлы, записанные на носители информации) и динамическая (пакеты, потоки, команды, запросы и др);
- 2) техническая инфраструктура: ИКТ, программное обеспечение, базы данных и базы знаний;
- 3) информационное взаимодействие субъектов с использованием полученной (переданной) информации и обработки через техническую инфраструктуру.

Как отмечалось выше, это понятие связывается Законом с понятием кибербезопасности как защищенностью «жизненно важных интересов человека и гражданина, общества и государства во время использования киберпространства».

На международном уровне используется ряд определений этого понятия, однако с учетом того, что обучение является видом деятельности, можно согласиться с подходом, согласно которому кибербезопасность рассматривается как «любая деятельность в сетевой, цифровой форме, включая содержание информации деятельность выполняется через цифровые сети» (Пряжников, 2018).

Учитывая, что сегодняшние школьники родились в цифровую эпоху, растут, учатся и развиваются в значительной степени именно в киберпространстве, можно утверждать, что киберпространство является и останется очень важной частью поля битвы идей и цивилизаций. Соответственно перед образованием встают новые задачи, связанные не только с формированием у соискателя образования необходимых знаний и социального самосознания, но и его понимание собственной интегрированности в мировое сообщество уже на ранних этапах обучения, практически неограниченных возможностей влияния киберпространства на свою личность, ответственности перед собой и обществом за свое поведение и ее (возможные) глобальные последствия, знания и понимание опасностей киберпространства.

Спектр опасностей от открытого киберпространства постоянно расширяется. Если десять лет назад опасности для учащихся школ можно было свести к относительно небольшому количеству групп – вирусные атаки, киберпреступность, опасности интернет-серфинга (Соколова, 2013), – то времени на разнообразие опасностей и угроз постоянно растет, затрагивая все возможные действия человека в сети. Наибольшую угрозу для школьников имеют скрытые активные опасности (Соколова, 2018).

Учитывая положения Федерального Закона “Об основных принципах обеспечения кибербезопасности” (Пряжников, 2018) сфера образования не входит в критические отрасли, на защиту которых направлен этот Закон. Однако сегодняшние ученики и студенты в короткие сроки могут работать в этих областях. Поэтому они уже сегодня нуждаются в защите и соответствующей подготовке, а также понимании общих возможных целевых групп кибербезопасности. Например, по такой классификации (Баликина, 2002):

- ученики / студенты,
- преподаватели,
- дети / молодежь,
- население (в целом, как социальная среда).

В зависимости от средств действия, проблемы (и соответствующие средства) кибербезопасности можно классифицировать по следующим группам (или уровням):

- правовые,
- технические,
- информационные, организационные,
- психологические.

Правовыми и техническими вопросами кибербезопасности занимаются специализированные специалисты и организации, поэтому они не рассматриваются в этой статье.

Информационные средства могут быть классифицированы в зависимости от задач, решаемых пользователями:

- защита / средства защиты,
- информирование,
- содержание,
- научиться использовать,
- безопасность,
- жизнестойкость, избегания угроз.

В широком смысле возможными целями воздействия кибербезопасности (кроме объектов критической инфраструктуры) могут быть:

- базы данных,
- персональные данные, среди которых финансовые,
- средства массовой информации,
- социальные сети,
- образование и профессиональная подготовка, учебники, историографические издания.

Организационные средства решения вопросов кибербезопасности:

- информирование,

- обучение культуре кибербезопасности, профессиональных работников КБ и населения в целом;
- создание специальных средств КБ,
- распространение средств КБ,
- контроль использования.

Психологические средства можно сгруппировать в зависимости от личностного и межличностного уровня:

- национальный,
- общественный,
- групповой,
- индивидуальный,
- культурный,
- когнитивный,
- интеллектуальный,
- привычки.

### **Заключение**

Хотя технологические решения разрабатываются в ответ на кибератаки, растет осведомленность о том, что роль человеческой деятельности и принятия решений в области кибербезопасности имеет решающее значение для повышения эффективности ответов на возникающие угрозы (Вацлавик, 2012). Особенно это важно с точки зрения будущей рабочей силы, поскольку молодежь является особенно чувствительной к внешнему воздействию и является наиболее активной частью сетевого населения".

Человеческий фактор может быть системным более слабым звеном, но в то же время также может быть мощным ресурсом для выявления и смягчения возникающих угроз.

### **Список литературы**

1. Антонова Л.Л., Полюшкевич О.А. Социокультурная безопасность и консолидация общества // Современные исследования социальных проблем (электронный научный журнал). 2012. №12 (20). С. 39.
2. Баликина, Г.В. Коммуникативное сопровождение мероприятий по модернизации образования / Г.В. Баликина, Б.Л. Рудник, А.А. Пинский, Г.В. Абонкина. М.: МО РФ, 2002. 12 с.
3. Васильева И.И., Соколова Н.Л., Михеева Н.Ф. Некоторые тренды использования ИКТ в российских научных исследованиях в области преподавания иностранных языков и перевода в ВУЗах (2012-2017) // Вопросы прикладной лингвистики. 2017. № 27. С. 7-18.
4. Вацлавик П. Психология межличностных коммуникаций / П. Вацлавик, Дж. Бивин, Д. Джексон. СПб.: Речь, 2012. 298 с.
5. Ведута Е.Н. Межотраслевой-межсекторный баланс: механизм стратегического планирования экономики: Учебное пособие для вузов. 2-е издание. М.: Академический проект. 2020. 239 с.
6. Гаджиева А.А. Учебное пособие (курс лекций) по дисциплине "Виктимология" для направления подготовки "Юриспруденция", профиль "Уголовное право". Махачкала: ДГУНХ.2016. 152 с.
7. Дубровский Д.И. Психические явления и мозг: Философский анализ проблемы в связи с некоторыми актуальными задачами нейрофизиологии, психологии, кибернетики / Отв.ред. А.Г. Спиркин. изд.2-е, доп. М.: ЛЕНАНД, 2021. 400 с.
8. Ломов Б.Ф. Общение как проблема общей психологии // Методологические проблемы социальной психологии. М.: Академический проект, 2012. С. 124-136.
9. Озерова М.М. Корпоративные коммуникации в управлении вузом: диссертация ... кандидата Социологических наук: 22.00.08. ФГАОУВО Белгородский государственный национальный исследовательский университет, 2017. 202 с.

10. Пряжников Н.С., Румянцева Л.С., Соколова Н.Л., Бахтигулова Л.Б. Профорентация: гармонизация точек зрения // Научный диалог. 2018. № 3. С. 289-303.
11. Соколова Н.Л. О компонентах значения единиц речевого этикета // Филологические науки. 2013. № 5. С. 95.
12. Соколова Н.Л. Профессиональная эволюция школьного педагога на базе передового педагогического опыта//Научный диалог. 2018. № 9. С. 376-381.
13. Соколова Н.Л. Тематическая группа «Знакомство» в англоязычной культуре общения // Вестник Московского государственного лингвистического университета. 2017. № 532. С. 218-227.
14. Vasbieva D.G., Sokolova N.L., Masalimova A.R., Shinkaruk V.M., Kiva-Khamzina Y.L. Exploring the efl teacher's role in a smart learning environment - a review study // XLinguae. 2018 . Т. 11. № 2. С. 265-274.

### Cybersecurity in a digital learning environment


#### **Alexandr S. Oleinik**

student

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

Moscow, Russia

sasha010698z@yandex.ru

 0000-0002-8021-3799


#### **Aleksey N. Shilov**

student

Far Eastern Federal University

Moscow, Russia

alexshow245@gmail.com

 0000-0000-0000-0000


#### **Danil A. Svetlichnyi**

student

Moscow State University of Civil Engineering

Moscow, Russia

danilsve4@gmail.com

 0000-0001-6559-4549


#### **Roman A. Makarov**

student

Moscow State University of Civil Engineering

Saint Petersburg, Russia

roma.makaro2001@yandex.ru

 0000-0001-6550-8751

#### **Anastasia A. Martazaeva**

student

Saint Petersburg University of Economics

Saint Petersburg, Russia


martazaeva.nacty@mail.ru

 0000-0000-0000-0000

Received 18.04.2022

Accepted 09.05.2022

Published 20.06.2022

 10.25726/f7435-3301-1451-c

### Abstract

People live and act in the digital space (CPU). Children are born, grow up, learn and will work with gadgets that are connected to networks and become a natural environment. Their life is influenced and influenced by the CPU with old and new dangers, depends more and more on cognitive factors, interface, content, behavior patterns) and can be characterized from the standpoint of safety, comfort efficiency (in particular health), that is, it is in the field of ergonomists. New problems arise caused by the life and activities in the Central Bank, the relevant factors of influence, ways to avoid them and the corresponding new means and tools. Accordingly, the problems of the development and implementation of information and communication technologies (ICT) in education that require solving, which is emphasized both at the international and national levels. However, it should be borne in mind that "under the influence of new information technologies, the processes of transformation of social development are so fundamental and global that, in addition to positive influence, they naturally bring with them serious problems, threats and risks in case of underestimation of new factors and conditions." As noted in the materials of the International Forums in Davos (2018-2019), the problem of cybersecurity (CB) is becoming particularly acute, which concerns almost all spheres of human life and activity, especially in conditions of full informatization of education. Due to cyber attacks, humanity suffers losses of more than 400 billion. US\$ per year.

### Keywords

cybersecurity, university, institute, protection.

### References

1. Antonova L.L., Poljushkevich O.A. Sociokul'turnaja bezopasnost' i konsolidacija obshhestva // *Sovremennye issledovanija social'nyh problem (jelektronnyj nauchnyj zhurnal)*. 2012. №12 (20). S. 39.
2. Balikina, G.V. Kommunikativnoe soprovozhdenie meroprijatij po modernizacii obrazovanija / G.V. Balikina, B.L. Rudnik, A.A. Pinskij, G.V. Abonkina. M.: MO RF, 2002. 12 s.
3. Vasil'eva I.I., Sokolova N.L., Miheeva N.F. Nekotorye trendy ispol'zovanija IKT v rossijskih nauchnyh issledovanijah v oblasti prepodavanija inostrannyh jazykov i perevoda v VUZah (2012-2017) // *Voprosy prikladnoj lingvistiki*. 2017. № 27. S. 7-18.
4. Vaclavik P. Psihologija mezhlichnostnyh kommunikacij / P. Vaclavik, Dzh. Bivin, D. Dzhekson. SPb.: Rech', 2012. 298 s.
5. Veduta E.N. Mezhotraslevoj-mezhsektornyj balans: mehanizm strategicheskogo planirovanija jekonomiki: Uchebnoe posobie dlja vuzov. 2-e izdanie. M.: Akademicheskij proekt. 2020. 239 s.
6. Gadzhieva A.A. Uchebnoe posobie (kurs lekcij) po discipline "Viktimologija" dlja napravlenija podgotovki "Jurisprudencija", profil' "Ugolovnoe pravo". Mahachkala: DGUNH.2016. 152 s.
7. Dubrovskij D.I. Psihicheskie javlenija i mozg: Filosofskij analiz problemy v svjazi s nekotorymi aktual'nymi zadachami nejrofiziologii, psihologii, kibernetiki / Otv.red. A.G. Spirkin. izd.2-e, dop. M.: LENAND, 2021. 400 s.
8. Lomov B.F. Obshhenie kak problema obshhej psihologii // *Metodologicheskie problemy social'noj psihologii*. M.: Akademicheskij proekt, 2012. S. 124-136.
9. Ozerova M.M. Korporativnye kommunikacii v upravlenii vuzom: dissertacija ... kandidata Sociologicheskikh nauk: 22.00.08. FGAOUVO Belgorodskij gosudarstvennyj nacional'nyj issledovatel'skij universitet, 2017. 202 s.
10. Prjazhnikov N.S., Rumjanceva L.S., Sokolova N.L., Bahtigulova L.B. Proforientacija: garmonizacija tocek zrenija // *Nauchnyj dialog*. 2018. № 3. S. 289-303.



11. Sokolova N.L. O komponentah znachenija edinic rechevogo jetiketa // Filologicheskie nauki. 2013. № 5. S. 95.
12. Sokolova N.L. Professional'naja jevoljucija shkol'nogo pedagoga na baze peredovogo pedagogicheskogo opyta//Nauchnyj dialog. 2018. № 9. S. 376-381.
13. Sokolova N.L. Tematicheskaja gruppa «Znakomstvo» v anglojazychnoj kul'ture obshhenija // Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. 2017. № 532. S. 218-227.
14. Vasbieva D.G., Sokolova N.L., Masalimova A.R., Shinkaruk V.M., Kiva-Khamzina Y.L. Exploring the efl teacher's role in a smart learning environment - a review study // XLinguae. 2018 . T. 11. № 2. S. 265-274.