Анализ внешних факторов, влияющих на кибербезопасность высшего военного учебного заведения

Александр Сергеевич Олейник
студент
Национальный исследовательский ядерный университет «МИФИ»
Москва, Россия
sasha010698z@yandex.ru
0000-0002-8021-3799

Татьяна Андреевна Якунина
студент
Национальный исследовательский Московский государственный строительный университет
Москва, Россия
tani_yakunina@mail.ru
0000-0003-0562-6208

Эльвира Ильдусовна Тагирова
студент
Национальный исследовательский Московский государственный строительный университет
Москва, Россия
t_elvira@inbox.ru
0000-0001-6365-1255

Алёна Васильевна Зыкова
студент
Нижегородский государственный университет имени Н.И. Лобачевского
Нижний Новгород, Россия
zykova.AB@gmail.com
0000-0000-0000-0000

Лилия Антоновна Щербаева
студент
Кубанский Государственный технический университет
Краснодар, Россия
lilia01.2001@gmail.com
0000-0000-0000-0000

Поступила в редакцию 19.04.2022
Принята 10.05.2022
Опубликована 20.06.2022

10.25726/c8003-8216-5580-l

Аннотация

Сейчас в России наблюдается активное внедрение ИКТ в образовательно-научную деятельность высших учебных заведений, в том числе и военных вузов (ВВУЗ). Соответственно, внедрение ИКТ в НЕМ является предпосылкой для большого потенциала изменений консервативных подходов относительно ежедневного обучения военнослужащих, что обусловлено его доступностью, мобильностью и эффективностью. В частности, 27 июня 2017 года состоялась кибератака с использованием

вредоносного программного обеспечения Petya, что повлекло нарушение функционирования государственных предприятий, учреждений, банков и медиа. Аналогично ухудшила состояние кибербезопасности в государстве – пандемия COVID-19. Так, вузы вынуждены были перейти на дистанционное обучение. С одной стороны, это ускорило внедрение ИКТ, а с другой – повысило угрозы в отношении кибератак со стороны злоумышленников, что опубликовано в соответствующих исследованиях ученых. Обусловлено это неготовностью и отсутствием в вузах практики по обеспечению кибербезопасности образовательно-научной деятельности в условиях удаленной работы.

Ключевые слова
анализ факторов, военный вуз, кибербезопасность.

Введение

Вместе с тем есть и проблемные вопросы по внедрению и применению ИКТ в ВВУЗ, а именно:

– недостаточное финансирование для закупки ИКТ;

– отсутствие стратегического видения со стороны руководства ВВУЗ по внедрению и применению современных ИКТ;

– недостаточная осведомленность преподавателей и обучаемых (студентов, солдат, курсантов и слушателей) по применению ИКТ во время обучения;

– отсутствие или наличие небольшого количества специалистов (непосредственно в ВВУЗЕ) которая бы обеспечивала функционирование и кибербезопасность ИКТ.В случае с тремя первыми пунктами по проблемным вопросам внедрения ИКТ в ВВУЗ, можно утверждать об активной деятельности руководителей ВВУЗ по их решению. Тогда как четвертый проблемный вопрос является крайне проблематичным и наблюдается не только в ВВУЗ но и на государственном уровне.

Причем, анализ научных публикаций свидетельствует, что наиболее распространенной кибератакой на образовательные ресурсы учебных заведений является DDoS атака, которая создавала трудности доступа к ним (Колесник, 2018; Литвин, 2020). Очевидно, что кибервлияние стало реальной угрозой и является одной из приоритетных проблем, как в повседневной жизни граждан, так и в образовательно-научной деятельности вуза. Поэтому актуальной является проблема обеспечения кибербезопасности вуза, в частности ВВУЗ, которые ежедневно осуществляют подготовку высококвалифицированных офицерских кадров и являются системообразующим элементом формирования и развития боеспособных и боеготовых Вооруженных Сил РФ.

Все более широкое внедрение ИКТ является сегодня общемировым явлением. Оно наблюдается практически во всех сферах человеческой деятельности, в том числе и военной (Колесник, 2018). Кроме того, современные процессы информатизации приводят как к повышению роли информационных технологий, так и в зависимости от них, в том числе в образовательно-научной деятельности ВУЗА.

Стоит отметить, что преимущественно все ВВУЗ прошли путь от консервативно-традиционного (учебно-научного) процесса к современной информационной (образовательно-научной) деятельности (Кузнецова, 2018). При этом, строительство собственного информационного пространства ВВУЗ включало, как правило такие шаги, а именно:

– обновление и модернизация ИКТ оборудования;

– разработка официального сайта ВУЗА и его структурных подразделений;

– подключение ВВУЗ к сети Интернет и создание собственной сети интранет;

– внедрение электронного документооборота;

– внедрение системы дистанционного обучения;

– разработка электронных образовательных ресурсов;

– разработка электронной библиотеки;

– внедрение системы электронных журналов для публикации научных результатов исследователей;

– внедрение системы видеоконференцсвязи;

– внедрение системы видеонаблюдения;

- автоматизация финансово-экономической деятельности ВВУЗ;
- автоматизация хозяйственной деятельности ВВУЗ;
- автоматизация кадровой деятельность ВВУЗ;
- автоматизация медицинской деятельности;
- внедрение системы контроля доступа к ВВУЗ.

Материалы и методы исследования

Следует отметить, что с одной стороны, за счет информатизации в НЕМ повышается качество и эффективность образовательно-научной деятельности, а с другой – создается многоуровневая информационно-пространственная система ВВУЗА, которая становится критическим объектом его надежного функционирования и кибербезопасности (Воронов, 2017).

Соответственно, под информационным пространством ВУЗА будем понимать – информационную среду (систему), которая образуется и функционирует в результате соединения различных по назначению ИКТ, с целью обеспечения субъект-субъектного взаимодействия того, кто учит, и того, кто учится.

При этом, под кибербезопасностью ВВУЗ будем понимать-состояние киберзащищенности информационного пространства ВВУЗ, при котором обеспечена конфиденциальность, целостность и доступность информации, которая в ней циркулирует.

Вместе с тем, критичность информационного пространства ВУЗА заключается в том, что в ней накапливается и циркулирует очень много конфиденциальной информации, а именно:

- персональная (данные постоянного и изменение состава ВВУЗ);
- служебная (директивы, приказы, распоряжения и документы с соответствующим грифом ограничения доступа);
- финансовая (финансовые отчеты и учет ресурсов);
- юридическое (судебные иски и служебные расследования);
- образовательно-научная (интеллектуальная собственность, патенты, перспективные научные изобретения, научно-исследовательские работы, образовательно-научные программы, профессиональные электронные журналы, электронные учебные курсы, электронная библиотека и электронные ресурсы).

В связи с этим, информационное пространство ВВУЗ является потенциальной целью для реализации различных кибератак со стороны злоумышленников (Просвирина, 2014) Кроме того, успешная реализация кибератаки на информационное пространство ВВУЗ может нанести такой вред:

- техническую (выход из строя технологического оборудования; блокирование доступа к информационному пространству заведения, в частности к образовательным ресурсам; уничтожение образовательно-научной (интеллектуальной) собственности);
- материальную (финансовые затраты на восстановление технологического оборудования; проведение аудита кибербезопасности экспертами частных фирм);
- репутационную (прекращение сотрудничества с другими вуза; снижение авторитета заведения; отток поступающих на обучение);
- моральную (шантаж руководства или сотрудников; задача стресса личности чьи данные были удалены, похищены или распространении).

Таким образом, вопрос обеспечения кибербезопасности ВВУЗ, приобретает особую важность и требует выполнения таких задач, а именно:

1. Анализа факторов, которые влияют на кибербезопасность ВВУЗА.
2. Разработка и внедрение модели киберзащиты ВВУЗ.
3. Оценка эффективности функционирования модели киберзащиты ВВУЗ.
4. Разработка рекомендаций по повышению эффективности функционирования модели киберзащиты ВВУЗА.

С учетом цели исследования, остановимся именно на первой задаче, а именно анализе факторов, влияющих на кибербезопасность ВВУЗ (Купряшин, 2020).

Стоит отметить, что кибербезопасность ВВУЗ взаимозависима от киберзащиты, который можно представить как комплекс взаимосвязанных мероприятий, которые образуют единое целое и имеют общую цель по обеспечению кибербезопасности ВВУЗ от влияния многих различных факторов (условий).

Следует отметить, что они могут по-разному влиять на кибербезопасность ВВУЗ, в частности одни из них могут иметь положительное влияние, другие же негативное (Часовских, 2017). Соответственно, доминирующее влияние негативных факторов способно снизить положительное действие других.

Внутренние факторы зависят от наших действий, поэтому мы можем влиять на их эффективность, как положительно, так и отрицательно.

То есть внутренние факторы могут как повысить кибербезопасность ВВУЗ, так и снизить ее через преднамеренные или непреднамеренные наши действия (Шмелькова6 2016).

Внешние факторы не зависят от нас, создаются внешними условиями или являются неконтролируемыми. Однако косвенно мы можем влиять на их эффективность путем усиления (усовершенствования своих внутренних факторов, которые направлены на обеспечение кибербезопасности ВВУЗА (Устюжанина, 2017).

Результаты и обсуждение

Соответственно, влияние внешних и внутренних факторов на кибербезопасность ВВУЗ определяет необходимость проведения постоянного мониторинга его состояния киберзащищенности. Безусловно, состояние киберзащищенности ВВУЗ будет зависеть от правильно смоделированной и реализованной модели киберзащиты, которая должна основываться на результатах анализа влияния внешних и внутренних факторов кибербезопасности ВВУЗ. (Свон, 2017)

Поэтому, анализ внешних и внутренних факторов помогает принять обоснованные управленческие решения, которые обеспечат взаимодействие ВУЗА с внешним информационным пространством в краткосрочной и долгосрочной перспективе. К тому же постоянный мониторинг и прогнозирование направления влияния (действия) внешних и внутренних факторов на кибербезопасность НЕМ, дает возможность руководству разрабатывать соответствующие стратегии реагирования, которые будут максимально адекватны ситуации, что может гипотетически произойти.

Следовательно, проведенный анализ кибербезопасности ВВУЗ позволяет определить такие основные внешние факторы, которые влияют на нее, а именно:

1. Чрезвычайные ситуации.
2. Разработка и производство аппаратно-программного обеспечения.
3. Кибератаки.
4. Вербовка или шантаж личного состава.

Соответственно, рассмотрим внешние факторы более подробно.

1. Чрезвычайные ситуации. ВВУЗ имеет определенное местоположение на отдельной территории, которая может подвергаться воздействию природной или техногенной опасности. При этом они могут возникать в комплексе, что значительно усиливает их воздействие. Возникновение одного опасного явления может вызвать ряд других (Ведута, 2017).

Естественная опасность. Любая деятельность или функционирование отдельного предмета, объекта или системы происходит во взаимодействии с естественной (окружающей) средой, в частности это воздух, вода, почва. Так же и информационное пространство ВВУЗ взаимодействует с природной средой своими отдельными элементами, а именно: информационно-телекоммуникационными системами, линиями связи, спутниковыми и Wi-Fi антеннами и т.д. (Зубарев, 2017) Соответственно, все они прямо или косвенно взаимодействуют с природной средой, которая может повлиять на их функционирование и состояние кибербезопасности ВВУЗ в целом, путем опасных природных явлений, в частности это:

- геологические (землетрясения, оползни, сель, карстовую пропасть, абразия);
- гидрологические (наводнения, паводки, подтопления, снежные лавины, дождь);

– метеорологические (град, жара, ветер, смерч, снегопад, мороз, молния).

Техногенная опасность. Масштаб техногенной опасности в НЕМ может достигать критического уровня, что связано с использованием электроэнергии, горючих, взрывоопасных веществ и материалов. Анализ техногенных ситуаций свидетельствует, что пожар или взрыв способны нанести значительные разрушительные потери как для критической информационной инфраструктуры, так и для личного состава ВВУЗА в целом. Поэтому, вопросу обеспечения техногенной безопасности следует уделять достаточно внимания, в частности устранить условия их возникновения (Косоруков, 2019).

2. Разработка и производство аппаратно-программного обеспечения.

Сейчас ИКТ с одной стороны обеспечивают повышение эффективности решения многих научно-прикладных задач, а с другой – втягивают в бесконечную зависимость от них все государственные институты страны, в частности ВВУЗ. Следует отметить, что основными составляющими ИКТ являются аппаратная и программная части.

Соответственно, аппаратная составляющая является технико-технологической основой (материнская плата, процессор, оперативное запоминающее устройство, графический адаптер, жесткий диск и т.д.), с помощью которой реализуется выполнения (функционирования) программной составляющей (операционные системы, разнообразное прикладное и системное программное обеспечение и т.д.). В связи с этим, они взаимозависимы и дополняют друг друга.

Следует отметить, что анализ применения аппаратно-программно обеспечения ВВУЗ свидетельствует, что оно иностранного разработки и производства. Кроме того, такая ситуация наблюдается во всех государственных институтах России.

Необходимо отметить, что связано это с возможностями нашей страны по разработке и производству соответствующих образцов аппаратно-программного обеспечения, в частности систематической нехваткой средств на финансирование соответствующих научно-технических разработок (Чумаченко, 2014). К тому же России будет трудно войти в круг разработчиков (монополистов) аппаратно-программного обеспечения, а необходимо с учетом времени и финансовых ресурсов – фантастические мечты.

Стоит отметить, что в настоящее время рынок аппаратно-программного обеспечения представлен такими участниками:

1. Intel Corporation (производит процессоры для различных цифровых систем и устройств США);
2. Advanced Micro Devices (производитель интегрированной электроники и второй крупнейший поставщик процессоров – США);
3. Nvidia Corporation (производитель графических процессоров, видеоадаптеров, мультимедийных и коммуникационных устройств для компьютеров – США);
4. Radeon Technologies Group (является подразделением Advanced Micro Devices, производит графические процессоры – США);
5. Microsoft Corporation (доминирующая корпорация по разработке программного обеспечения, ее продуктами пользуются и домашние пользователи, и международные корпорации – США);
6. Oracle Corporation (разработчик программного обеспечения и баз данных для организаций – США);
7. Red Hat (компания выпускает программные решения на базе свободной операционной системы GNU / Linux – США);
8. The Debian Project (проект разработчика программного обеспечения Иана Эшли Мердока – США);
9. Cisco Systems, Inc Cisco Systems (мировой лидер в области сетевых технологий – США);
10. Dell-американская корпорация, одна из крупнейших компаний в области производства компьютеров – США);
11. Hewlett-Packard (поставщик аппаратного и программного обеспечения для организаций и индивидуальных потребителей – США);

12. International Business Machines (один из крупнейших во всем мире производителей и поставщиков аппаратного обеспечения - США);

13. Western Digital (производитель компьютерной электроники – США);

14. Toshiba (международный концерн, работающий в области электротехники и электроники – Япония);

15. D-Link (поставляет сетевые и коммуникационные решения предприятиям, малому и среднему бизнесу, Интернет провайдерам и компаниям, предоставляющим услуги связи – Тайвань).

С учетом вышесказанного, возникает необходимость определения ключевых особенностей влияния иностранного программного обеспечения на кибербезопасность ВВУЗА, которые заключаются в следующем:

1) во-первых, ошибки при разработке и производстве аппаратно-программного обеспечения (отсутствие возможности контроля производства и тестирования аппаратно-программного обеспечения, что может привести к нештатным ситуациям во время его функционирования, в частности к полному или частичному выводу из строя);

2) во-вторых, отсутствие юридической ответственности за отсутствие киберзащиты при разработке и производстве аппаратно-программного обеспечения (ответственность за потенциально возможные реализованы кибератаки или сбои лежит исключительно на пользователе, который его обслуживает);

3) в-третьих, гипотетическая вероятность наличия намеренно встроенных уязвимостей в аппаратно-программном обеспечении (переход от классических боевых действий в информационное противоборство, где вопросы своих национальных интересов всегда будет стоять выше интересов других стран);

4) в-четвертых, невозможность создания единой системы киберзащиты ВВУЗА в соответствии с предложенных решений со стороны иностранного производителя аппаратно-программного обеспечения (наличие желания создания комплексной системы киберзащиты ВВУЗ и отсутствие финансовых возможностей для ее реализации, в частности высокая цена – высокий уровень киберзащищенности, низкая цена – низкий уровень киберзащищенности ВВУЗА).

А значит, без сомнения можно сказать, что все аппаратно-программное обеспечение которое используется в ВВУЗ является иностранного производства, а это увеличивает вероятность его влияния на кибербезопасность ВВУЗ.

3. Кибератаки. Следует отметить, что одним из главных факторов, который влияет на кибербезопасность ВВУЗ является кибератака. Под кибератакой будем понимать-целенаправленные действия на составные элементы информационного пространства, которые выполняются путем применения аппаратно-программных средств с целью нарушения их конфиденциальности, целостности и доступности.

К тому же кибератака может выполняться удаленно (нахождение атакующего за пределами операционной зоны воздействия по отношению к объекту) или локально (непосредственное физическое присутствие атакующего по отношению к объекту воздействия).

В основном самыми распространенными типами кибератак, которые наблюдаются являются:

– вредоносное программное обеспечение (в зависимости от его функционала может получить полный доступ к операционной системе, в частности: контролирование действий объекта воздействия и нажатия клавиш; отправка, уничтожение или модификация конфиденциальной информации и т.д.);

– фишинг (использование заинтересованности или импульсивности объекта воздействия с целью выполнения им заранее спланированных опасных действий, в частности: открытия в электронном письме ссылки или файла, что приведет к заражению или перенаправления на вредоносный сайт; использование коротких текстовых сообщений (смишинг) или голосовых вызовов (вишинг) с целью выполнения описанных выше действий по отношению к объекту воздействия);

– SQL Injection (применение языка структурированных запросов для воздействия на базу данных сайта (сервера) объекта воздействия, что позволяет выполнять вредоносный код);

– XSS (межсайтовый скриптинг, что позволяет использовать уязвим сайт (сервер) для кибератаки на объект воздействия, в том числе вредоносный код интегрируется в сайт, который будет посещать объект воздействия, что в дальнейшем позволяет атакующему получить его авторизационные куки);

– DoS (отказ в обслуживании, которая заключается в невозможности получить доступ к информационному ресурсу (объекту атаки) в связи с одновременным подключением к нему сети ботов, что приводит к полной расходы памяти и процессорного ресурса сервера);

– атака нулевого дня (использование уязвимости аппаратно-программного обеспечения, которая неизвестна его пользователям или разработчикам, что позволяет атакующему использовать ее в своих намерениях, с целью нарушения конфиденциальности, целостности и доступности информационного ресурса).

Вербовка или шантаж личного состава. В последние годы очень много говорится о деятельности российской агентуры в России, в частности резонанс был с задержанием высокопоставленных чиновников. Эти случаи свидетельствуют, что активно происходит вербовка или шантаж соответствующих субъектов с целью причинения вреда национальной безопасности России.

Кроме того, гипотетически это может произойти и в ВВУЗ, который выполняет важную задачу по подготовке высококвалифицированных офицерских кадров и является системообразующим элементом формирования и развития боеспособных и боеготовных Вооруженных Сил России.

В связи с этим встает очень сложная задача по недопущению вербовки должностных лиц (отвечают за функционирование информационной инфраструктуры) и постоянного личного состава (профессорско-преподавательский состав) ВВУЗА, которые потенциально могут быть завербованы или под влиянием шантажа выполнить кибератаки на критические элементы информационного пространства ВУЗА.

Заключение

Проанализировав внешние факторы, которые влияют на кибербезопасность ВВУЗА можем сделать вывод, что они являются неконтролируемыми со стороны ВВУЗА, а также под их влиянием возникает необходимость изменять и усиливать свои внутренние факторы, которые с одной стороны уменьшают эффективность влияния внешних факторов, а с другой – обеспечивают кибербезопасность ВВУЗА. В то же время есть необходимость анализа внутренних факторов, которые влияют на кибербезопасность ВВУЗ.

Список литературы

1. Ведута Е.Н., Джакубова Т.Н. Big Data и экономическая кибернетика // Государственное управление. Электронный вестник. 2017. № 63. С. 43-66.
2. Воронов М.П., ЧасовскихВ.П. Blockchain – основные понятия и роль в цифровой экономике // Фундаментальные исследования 2017. № 9. С. 30-35.
3. Зубарев А.Е. Цифровая экономика как форма проявления закономерностей развития новой экономики // Вестн. ТОГУ 2017. № 4 (47). С. 177-184.
4. Колесник А.П. Социальные системы в цифровой экономике // Стратегии бизнеса. 2018. № 1 (45). С. 3-11.
5. Косоруков А.А. Роботизация в контексте цифровой трансформации государственного управления в Российской Федерации // Вопросы политологии. 2019. Т. 9. № 11 (51). С. 2388-2397.
6. Кузнецова В.П., Бондаренко И.А. Блокчейн как инструмент цифровой экономики в образовании // Journal of Economic Regulation. 2018. Т. 9. № 1. С. 102-109.
7. Купряшин Г.Л., Шрамм А.Е. О проблемах информатизации в бюрократических системах и развитии общегосударственных информационных систем // Государственное управление. Электронный вестник. 2020. № 80. С. 22-48. URL:
8. Литвин А.А., Коренев С.В., Князева Е.Г. Современные возможности использования технологии блокчейн в системе образования // Развитие образования. 2020. № 3 (9). С. 107-114.

9. Просвирина И.И., Тащев А.К. Экономика знаний и современные тенденции использования труда в России // Вестн. Южно-Уральского гос. ун-та. Сер.: Экономика и менеджмент. 2014. Том 8. № 1. С.73-77.
10. Свон М. Блокчейн: схема новой экономики. М.: Издательство «Олимп-Бизнес», 2017.
11. Устюжанина Е.В., Сигарев А.В., Шеин Р.А. Цифровая экономика как новая парадигма экономического развития // Национальные интересы: приоритеты и безопасность. 2017. Т. 13, № 10. С. 1788-1804.
12. Часовских В.П., Лабунец В.Г., Воронов М.П. Технология «Блокчейн» (blockchain) в образовании вузов и цифровой экономике // Эко-потенциал, 2017. № 2 (18). С. 99-105.
13. Чумаченко Н.Э. Информационная экономика и новая экономика: общее и особенное, понятийный аппарат и содержание // Вестн. Саратовского гос. социально-экономического ун-та. 2014. № 3 (52). С. 35-39.
14. Шмелькова Л.В. Кадры для цифровой экономики: взгляд в будущее // Дополнительное профессиональное образования в стране и мире. 2016. № 8 (30). С.1-4.

Analysis of external factors affecting the cybersecurity of a higher military educational institution

Alexandr S. Oleinik
student
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Moscow, Russia
sasha010698z@yandex.ru
0000-0002-8021-3799

Tatyana A. Yakunina
student
Moscow State University of Civil Engineering
Moscow, Russia
tani_yakunina@mail.ru
0000-0003-0562-6208

Elvira I. Tagirova
student
Moscow State University of Civil Engineering
Moscow, Russia
t_elvira@inbox.ru
0000-0001-6365-1255

Alena V.Zykova
student
N. I. Lobachevsky State University of Nizhny Novgorod
Nizhny Novgorod, Russia
zykova.AB@gmail.com
0000-0000-0000-0000

Lilia A. Scherbaeva
student
Kuban State Technological University
Krasnodar, Russia
lilia01.2001@gmail.com
0000-0000-0000-0000

Received 19.04.2022
Accepted 10.05.2022
Published 20.06.2022

10.25726/c8003-8216-5580-l

Abstract

Now in Russia there is an active introduction of ICT in the educational and scientific activities of higher educational institutions, including military universities (VVUZ). Accordingly, the introduction of ICT in IT is a prerequisite for a large potential for changes in conservative approaches regarding the daily training of military personnel, which is due to its accessibility, mobility and efficiency. In particular, on June 27, 2017, a cyberattack using malicious Petya software took place, which caused disruption of the functioning of state-owned enterprises, institutions, banks and media. Similarly, the COVID–19 pandemic worsened the state of cybersecurity in the state. Thus, universities were forced to switch to distance learning. On the one hand, this accelerated the introduction of ICT, and on the other hand, increased the threat of cyber attacks from intruders, which is published in relevant research by scientists. This is due to the unavailability and lack of practice in universities to ensure the cybersecurity of educational and scientific activities in the conditions of remote work.

Keywords

factor analysis, military university, cybersecurity.

References

1. Veduta E.N., Dzhakubova T.N. Big Data i jekonomicheskaja kibernetika // Gosudarstvennoe upravlenie. Jelektronnyj vestnik. 2017. № 63. S. 43-66.
2. Voronov M.P., ChasovskihV.P. Blockchain – osnovnye ponjatija i rol' v cifrovoj jekonomike // Fundamental'nye issledovanija 2017. № 9. S. 30-35.
3. Zubarev A.E. Cifrovaja jekonomika kak forma projavlenija zakonomernostej razvitija novoj jekonomiki // Vestn. TOGU 2017. № 4 (47). S. 177-184.
4. Kolesnik A.P. Social'nye sistemy v cifrovoj jekonomike // Strategii biznesa. 2018. № 1 (45). S. 3-11.
5. Kosorukov A.A. Robotizacija v kontekste cifrovoj transformacii gosudarstvennogo upravlenija v Rossijskoj Federacii // Voprosy politologii. 2019. T. 9. № 11 (51). S. 2388-2397.
6. Kuznecova V.P., Bondarenko I.A. Blokchejn kak instrument cifrovoj jekonomiki v obrazovanii // Journal of Economic Regulation. 2018. T. 9. № 1. S. 102-109.
7. Kuprjashin G.L., Shramm A.E. O problemah informatizacii v bjurokraticheskih sistemah i razvitii obshhegosudarstvennyh informacionnyh sistem // Gosudarstvennoe upravlenie. Jelektronnyj vestnik. 2020. № 80. S. 22-48. URL:
8. Litvin A.A., Korenev S.V., Knjazeva E.G. Sovremennye vozmozhnosti ispol'zovanija tehnologii blokchejn v sisteme obrazovanija // Razvitie obrazovanija. 2020. № 3 (9). S. 107-114.
9. Prosvirina I.I., Tashhev A.K. Jekonomika znanij i sovremennye tendencii ispol'zovanija truda v Rossii // Vestn. Juzhno-Ural'skogo gos. un-ta. Ser.: Jekonomika i menedzhment. 2014. Tom 8. № 1. S.73-77.
10. Svon M. Blokchejn: shema novoj jekonomiki. M.: Izdatel'stvo «Olimp-Biznes», 2017.

11. Ustjuzhanina E.V., Sigarev A.V., Shein R.A. Cifrovaja jekonomika kak novaja paradigma jekonomicheskogo razvitija // Nacional'nye interesy: prioritety i bezopasnost'. 2017. T. 13, № 10. S. 1788-1804.
12. Chasovskih V.P., Labunec V.G., Voronov M.P. Tehnologija «Blokchejn» (blockchain) v obrazovanii vuzov i cifrovoj jekonomike // Jeko-potencial, 2017. № 2 (18). S. 99-105.
13. Chumachenko N.Je. Informacionnaja jekonomika i novaja jekonomika: obshhee i osobennoe, ponjatijnyj apparat i soderzhanie // Vestn. Saratovskogo gos. social'no-jekonomicheskogo un-ta. 2014. № 3 (52). S. 35-39.
14. Shmel'kova L.V. Kadry dlja cifrovoj jekonomiki: vzgljad v budushhee // Dopolnitel'noe professional'noe obrazovanija v strane i mire. 2016. № 8 (30). S.1-4.