Санкт-Петербургский государственный университет

ЕРЕМИН Даниил Николаевич

Выпускная квалификационная работа

*Обеспечение информационной безопасности Ленинградской области в рамках реализации политики цифровизации*

Уровень образования: бакалавриат

Направление 41.03.04 «Политология»

Основная образовательная программа СВ.5027\* «Политология»

Научный руководитель:

доц. каф. политического управления

док. политических наук

Волкова Анна Владимирова

Рецензент:

Первый заместитель Председателя Комитета

начальник департамента

Комитета цифрового развития Ленинградской области

Хомичев Евгений Александрович

Санкт-Петербург

2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3

Глава I Теоретические основания политики цифровизации: зарубежный опыт и российские реформы 7

1.1 Цифровизация с позиции политической науки 7

1.2 Реализация политики цифровизации в Российской Федерации: опыт регионов 15

1.3 Основные доктрины информационной безопасности и политика цифровизации 22

Глава II Цифровизация и развитие кадрового потенциала в Ленинградской области: вызовы и перспективы 27

2.1 Основные потребности рынка труда и государственных органов в сфере цифровизации и информационной безопасности 27

2.2 Развитие рынка образовательных программ в сфере цифровизации и информационной безопасности. 35

Глава III Опыт реализации политики информационной безопасности в Ленинградской области 42

3.1 Проект «Территория Безопасности» как пример общественной иниицативы в сфере информационной безопасности 42

3.2 Работа государственных органов по обеспечению информационной безопасности в Ленинградской области 50

ЗАКЛЮЧЕНИЕ 57

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 60

ПРИЛОЖЕНИЯ 65

ВВЕДЕНИЕ

Процесс управления публичной политикой и оценка его эффективности в начале XXI в. характеризуется целым рядом новых черт, которые активно анализируются обществоведами всего мира. Современные государства столкнулись с новейшими вызовами, наиболее значимый из которых, - кризис управляемости, обусловленный как растущими требованиями со стороны общества к правительствам в условиях «сетевизации» управления, так и нарастанием глобальных проблем, как например комплекс вызовов, связанных с пандемией COVID 19.

Российские реформы в сфере государственного управления на рубеже веков были обусловлены множеством факторов, и рыночной ориентацией политических элит. Понятие «качество управления», получившее распространение в связи с менеджериальными реформами конца ХХ в., сегодня включает целый ряд понятий (прозрачность, безопасность, комфорт, доступность и др.) и выступает (как и «уровень жизни») значимым показателем для оценки условий жизни населения. С другой стороны, использование новых форм координации взаимодействий граждан, бизнес-структур и государства в экономике и политике, основанных на цифровых технологиях, порождает специфические проблемы и новые вызовы. Так, к примеру, часто встречающаяся трактовка цифровизации, как технико-технологического переоснащения управленческих структур, не позволяет оценить все преимущества сетевых платформ взаимодействия, как, впрочем, и социальные риски, связанные с их внедрением. Действительно, изначально задуманная, как способ совершенствования системы государственного управления цифровизация превратилась во всеобъемлющий фактор реформирования социальных институтов и если в начале XXI в. цифровое развитие рассматривалось как перспективное направление совершенствования государственного управления, то сегодня цифровизация и новейшие способы коммуникации являются для нас данностью. Web 2.0, интернет вещей, машинное обучение, искусственный интеллект стали неотъемлемой частью нашей жизни. Развитие способов коммуникации, появление новейших видов СМИ сформировали эпоху постправды. Публичная политика и государственное управление должны были принять новейшие вызовы времени и развиваться в соответствии с ними.

Одним из наиболее дискуссионных проблем возникших при цифровизации стало обеспечение безопасности. Новейшие технологии поставили под угрозу интеллектуальную собственность граждан, их права на свободу, свободу слова и свободу частной жизни. Сформированный еще в XX в. концепт информационной безопасности обрел новое понимание, связанное с развитием ИКТ и Интернета. Обеспечение информационной безопасности стало одним из важнейших направлений при осуществлении политики цифровизации. Создание инфраструктуры, обеспечение безопасности каналов передачи данных и серверов хранения информации стало обязательной составляющей цифровой политики государств.

Актуальность данной работы обусловлена большим интересом российского Правительства к национальной программе «Цифровая экономика», рассматривающийся как один из наиболее прогрессивных за последние года. Крупномасштабная политика по цифровизации регионов, запущенная в 2018 году, привлекла не только огромные финансовые вливания со стороны федерального бюджета и частных компаний, но и стала важной составляющей публичной политики. Информационная безопасность - один из наиболее важных для российского Правительства пунктов данной национальной программы. Информационная безопасность регионов - прямое продолжение инициатив по созданию суверенного российского сегмента Интернета и политике по охране больших данных страны. Ленинградская область - один из наиболее продвинутых в цифровой среде регионов, он является одним из лидеров по внедрению новейших цифровых технологий в государственное управление.

Теоретическое осмысление влияния новых коммуникационных технологий мы находим у М. Кастельса ( концепция сетевого общества), М. Маклюэна (концепция символического капитала в новых технологиях), Дж.Нэсбит и П. Эбурдин ( электронная демократия), Е. Масуда (появление информационных сообществ). Среди отечественных исследователей данной темы стоит выделить Акцент в отечественных исследованиях сделан на сетевой характер взаимодействия, среди исследователей по данной теме Т.А. Кулакова, И.В Мирошниченко, И.В. Самаркина, а так же влияние развития интернета на политический процесс - А. В. Чугунов. А.В. Волкова в своих работах соотносит цифровое развитие и электронное правительство с формированием новых публичных ценностей. Стоит также выделить работы Л.В. Сморгунова о цифровизации как о факторе изменения социальных институтов и перехода к сотрудничеству в сфере государственного управления между государством, бизнесом и гражданами.

В данной работе информационной безопасность в политике цифровизации будет рассматриваться с позиции неоинституционализма, то есть понимания публичной политики не только как поля деятельности исключительно государственных структур, сколько площадка для взаимодействия различных акторов государства, бизнеса и граждан. В том числе автор опирается на концепцию «Good governance» ( «хорошего управления») , как одну из наиболее влиятельных на сегодняшний день в сфере государственного управления.

Объект исследования - политика по обеспечению информационной безопасности.

Предмет исследования - Обеспечение информационной безопасности процессе цифровизации систем управления Ленинградской областью.

Рабочая гипотеза исследования: Цифровизация, в основе которой лежит техническое совершенствование средств коммуникации, на деле затрагивает и изменяет социальную и политическую структуру общества, обуславливая различия в подходах к обеспечению информационной безопасности.

Целью данной работы является анализ подходов к обеспечению информационной безопасности в Ленинградской области в условиях цифровизации в контексте проблемы повышения качества жизни населения.

А также ставит перед собой следующие задачи:

* Рассмотреть теоретические основания цифрового развития региона.
* Проанализировать темпы цифрового развития России и Ленинградской области.
* Выявить основные направления работ по обеспечению информационной безопасности в России и регионе.
* Установить требования рынка труда в сфере информационной безопасности и требования, выдвигаемые на государственной гражданской службе Ленинградской области в условиях цифрового развития.
* Проанализировать образовательные программы ведущих ВУЗов по подготовке кадров для обеспечения информационной безопасности и подготовки государственных служащих.
* Установить основные направления по обеспечению информационной безопасности специализированных структурных подразделений Правительства Ленинградской области.
* Проанализировать социальные проекты, поддержанные Правительством Ленинградской области в сфере информационной безопасности.

Глава I Теоретические основания политики цифровизации: зарубежный опыт и российские реформы

1.1 Цифровизация с позиции политической науки

Во второй половине XX века начинает складываться теория о переходе общества от индустриального уклада к постиндустриальному. Два основных направления, разграничивающих взгляды на данную теорию - идея «программируемого общества» А. Турена и «информационное общества» Ф.Махлупа.[[1]](#footnote-1)

Основным посылом перехода к постиндустриальному укладу становится смещение акцентов на коммуникацию и технологии коммуникации, которые должны будут изменить структуру общества, политических институтов и способы политического управления.[[2]](#footnote-2) Структура общества под влияние коммуникационных технологий изменяется на сетевую. Подобное изменение структуры делает коммуникацию массовой.[[3]](#footnote-3)

Современные политические процессы все больше диктуют нам необходимость в освоении и внедрении новейших цифровых технологий. Скорость коммуникации и принятия решений возросла до огромных масштабов. Технологический прорыв дал новый толчок к развитию принципов открытости, сотрудничества и инноваций. Как не парадоксально вместе с принципами открытости цифровизация обострила проблему личной свободы и контроля государства.

«Цифровизация публичного управления часто понимается как процесс использования новых ИКТ и в особенности электронных технологий для организации и обеспечения эффективного функционирования публичной сферы. При этом подчеркивается, что цифровизация в политическом смысле – это способ расширить политические формы взаимодействия общества и государства, сделав публичное управление совместным»[[4]](#footnote-4) То есть нельзя понимать цифровизацию как исключительно введение новейших цифровых технологий, в политике это в первую очередь возможность расширить взаимодействие государства с частным сектором и гражданами, то есть трансформировать государственное управление в формат «достойного управления».

Проблема усиления контроля государства за гражданами с использованием новейших технологий все больше поднимается в связи с политикой цифрового развития, цифровые технологии помимо открытости приобретают характер инструмента за контролем над гражданского обществом и частной жизнью.[[5]](#footnote-5) Появившаяся возможность отслеживания массива Больших данных дает почти безграничные возможности для мониторинга возможных угроз и правонарушений внутри государства. Огромные корпорации вроде Google и Facebook знают о нас зачастую намного больше, чем нам кажется.[[6]](#footnote-6)

В настоящее время в науке используются два основных подхода к политике цифровизации в государственном управлении: концепция нового государственного управления ( public management) и концепция «достойного управления (управляемости)» (good governance). Новое государственное управление понимает государство как систему сервисных функций, соответственно, деятельность государственных служащих - оказание услуг, а достойное управление как переход от понимания управления как исполнения функций к управлению как сети взаимосвязей государства и граждан: граждане участвуют в принятии политических решений, негосударственные организации и объединения представлены в государственном управлении.[[7]](#footnote-7)

Теоретики государственного управления полагают, что цифровое управление может основываться на сотрудничестве и прозрачности, то есть отношения между государством и гражданами будут определяться обезличенными алгоритмами цифровых технологий, что позволит свести на нет постоянные взаимные недоверия и споры. Правда, стоит отметить, что одна из потенциально важнейших проблем обезличенных алгоритмов, это проблема «создателя». Тот, кто создает алгоритмы, определяет правила игры, а они не обязательно могут отвечать принятым критериям справедливости.

Государственное управление в эпоху цифровых технологий ассоциируется в первую очередь с «электронным правительством». Электронное правительство в данном контексте понимается как простая информатизация и автоматизация государственного сектора, электронное правительство ориентировано на ценности государства, а не общества.[[8]](#footnote-8) То есть основной задачей государства в политике цифровизации выступает информирование население, оказание услуг с помощью интернет-порталов. На деле же этот подход уже является чересчур узким.[[9]](#footnote-9) Узкий подход к цифровизации позволяет лишь повысить уровень предоставления государственных услуг.

В более широком смысле цифровизация позволяет изменить существующий подход к государственному управлению. В данном случае подразумевается расширение участия граждан, совместное решение общественных проблем заинтересованными сторонами, определение повестки дня. И на данном этапе политика цифровизации выходит за свои рамки и трансформирует государство. Государство больше не является основным и единственным институтом принятия решений.[[10]](#footnote-10) Государство превращается в регулятор межчеловеческого взаимодействия, отдавая право принятия решений на более низкий уровень. Без цифровых технологий подобное было невозможно представить, поскольку отсутствовали необходимо каналы коммуникации. А на сегодня принятие общественного решения без вмешательства государства с помощью цифровых технологий кажется почти реальностью.

Как уже было сказано выше государство получает в свои руки инструмент за контролем сверху. В условиях широкого использования Больших данных государство получает не только возможность контроля за личными данными гражданами, но также и возможность к использованию этих данных в своих интересах, то есть цифровые технологии становятся инструментом политического манипулирования.

При этом существует и контроль снизу. Цифровые технологии вызвали ответную реакцию у гражданского общества, выразившегося в социальном самоконтроле. Подобный контроль снизу выражается не только в размещении своих персональных данных в социальных сетях, но также и предоставления публичного доступа к записям средств видеоконтроля. Объясним подробнее, при контроле сверху главенствующую роль играет государство, оно занимается организацией дисциплинарного пространства. При контроле же снизу ответственными за организацию становятся все участники. Соответственно именно от контроля снизу проистекают такие требования, как равенство в доступе к информации и прозрачности. Равенство позволяет каждому наблюдать, а значит и контролировать остальных. Мы оказываемся в условиях, когда все знают все о каждом.[[11]](#footnote-11)

Условием появления обоих видов контроля стали безопасность и эффективность. Одним из первых толчков к внедрению цифровых технологий в начале 2000-х стала борьба с терроризмом. Государственные органы стали переходить к новому режиму безопасности, основанному на технологических инновациях. Использование Больших данных позволило осуществлять мониторинг и превентивную деятельность в сфере безопасности.

Вторым важным толчком к внедрению цифровых технологий стала потребность в повышении эффективности оказания публичных услуг государством, что в том числе влияло и на положительный имидж государственных структур.

Стоит отметить также и то, что внедрение новейших технологий наблюдается не только в демократических странах, но и в авторитарных. Демократические страны не могут избежать подобных нововведений из-за необходимости повышения как эффективности управления, так и безопасности. Авторитарные режимы также используют новейшие цифровые технологии для тех же потребностей, лишь по-другому расставляя приоритеты, в первую очередь здесь имеется ввиду курс на легитимизацию самого режима.

Важной составляющей цифровизации политики государственного управления является наличие условий для гармоничного взаимодействия государства и граждан. Важным пунктом данных условий является ограничение контроля сверху с помощью использования криптографических алгоритмов. Так же важным средством обеспечения гармоничного взаимодействия является нормативное разграничение полномочий, а так же ограничение дисциплинарного пространства для контроля сверху. Государство имеет право контролировать определенную часть цифрового мира, но не должно вмешиваться в частную жизнь. Условно говоря, контроль за открытыми данными в социальных сетях возможен, а контроль за личной перепиской нет.

Одним из самых интересных следствий цифровизации является возможность возрождения институтов прямой демократии. Это интересно потому, что демократия находится в очередном кризисе. Людей разочаровывают демократические процедуры, они зачастую не обеспечивают обещанную и гарантированную конституцией справедливости и равенства. Институт прямой демократии отмирал постепенно с увеличением политических единиц. Увеличение числа участников в принятии решения напрямую противоречила возможностям прямой демократии. Прямая демократия возможна для 10, 100, 1000 участников. Но как реализовать прямую демократию в условиях, когда в государстве, например, 145 миллионов человек? Ответом на старый вопрос стала цифровизация и новейшие способы коммуникации.

ИКТ первых трех поколений определили функциональную (услуги электронного правительства), организационную (электронное участие) и коммуникативную (мониторинг демократии) задачи государственного управления. ИКТ четвертого поколения явила миру технологию распределения баз данных, блокчейн. Появилась радикальная концепция «управления без правительства.[[12]](#footnote-12) Общество может управляться без вмешательства государственных структур на основе доверительности обезличенным цифровым протоколам. Блокчейн позволяет совершать транзакции на основе криптографических протоколов без доверия или без участия третьих лиц. Важнейшим преимуществом подобной структуры для управления выступает децентрализация, прозрачность, снижение расходов. Подобные инновации определили существующие административные и политические реформы. В политике цифровизации происходит переход от узкого подхода к широкому, о которых мы говорили выше. Сугубо узкое направление электронного правительства постепенно сменяется оказанием услуг и принятием решений с участием граждан. От концепции государственного управления, как контроля, мы переходим к концепции сотрудничества. Государство и граждане совместно определяют направления деятельности. Таким образом, цифровые технологии позволяют частично возродить институт прямой демократии с упором на новейшие способы коммуникации.

Цифровизация является не только способом повышения эффективности оказания услуг и повышения безопасности. Цифровизация выходит за рамки исключительно государственного управления. Она позволяет расширить возможности взаимодействия граждан и государства. Цифровые технологии позволяют решить актуальную проблему представительной демократии, привлечь к решению общественных проблем большее число участников-граждан. Блокчейн создает возможность для процессуальной справедливости[[13]](#footnote-13), что является одним из самых слабых мест сегодняшних демократий. Криптография позволяет наметить доверие не только между гражданами и государством, но и между участниками мировой политики.[[14]](#footnote-14)

В международных отношениях все больше встает вопрос о защите цифрового суверенитета. Понятие «Суверенный интернет» из парадоксально невозможного становится обыденным. Государства в условиях цифровизации все больше озабочены проблемами национальной безопасности. охраны национальных больших данных. Если раньше государство никак не вмешивалось в отношения в Интернете, то сегодня все больше участников настаивают на необходимости контроля за интернетом.[[15]](#footnote-15) Государства все больше стараются контролировать потоки в Интернете и стремиться обезопасить себя с помощью новейших технологий. В мире наблюдается рост цифрового авторитаризма.

Подводя итог, цифровизация политики выходит за рамки государственного управления. Новейшие цифровые технологии стали внедряться в структуру государственного управления из соображений безопасности и эффективности оказания услуг.

На сегодняшний день наблюдается контроль за цифровым развитием сверху и снизу. Государство, используя новейшие технологии создает дисциплинарное пространство, в котором оно может контролировать персональные данные граждан. Существует так проблема увеличения контроля государства за жизнью граждан, а также необходимость ограничения подобного контроля от вмешательства в частную жизнь. Контроль снизу подразумевает всеобщую гласность, когда пользователи самостоятельно выкладывают информацию о себе в интернет, а взамен получают доступ к персональной информации других пользователей.

Цифровизация позволяет не только улучшить качество существующих услуг, одной из важнейших задач для нее является расширение участия граждан в принятии решений.

Узкий подход, который заключается в оптимизации и повышении эффективности государственного управления, имеет свои недостатки и не описывает всю полноту возможностей, которые дает цифровизация. Широкий подход заключается в расширении взаимодействия, сотрудничества государства и граждан. Таким образом, речь идет уже не об улучшении, а о эволюции демократического режима в целом. Сегодня мы получаем инструмент для развития прямой демократии в условиях огромного общества.

1.2 Реализация политики цифровизации в Российской Федерации: опыт регионов

В России на протяжении длительного периода представители власти «пытаются разрешить базовый конфликт, определяемый тенденцией к авторитаризму, с одной стороны, и слабой эффективностью методов управления – с другой»[[16]](#footnote-16) Повышение эффективности государственного управления становится одним из приоритетных направлений в политических исследованиях. В современной России наблюдается выделение информационной среды в особую модернизационную зону, в первую очередь за счет обоснования стратегического значения цифровизации для современного государства.

Цифровизация в России крупномасштабно стартовала в 2017 году после обращения Президента к Федеральному собранию. Основные цели России по цифровизации заключены в государственной программе «Цифровая экономика», затем ставшей основной одноименного национального проекта.

Перед тем как мы перейдем к рассмотрению внутренней российской политики цифровизации, необходимо рассмотреть положении России в мировых рейтингах цифровизации, чтобы понимать общую картину.

Согласно Индексу развития ИКТ на 2017 год, то есть на момент старта программы, Россия находилась на 45 месте (Приложение 1). Согласно одному из самых популярных на 2015 г. индексов BCG e-Intensity Россия так же была далеко не в лидерах по цифровизации и занимала 39 место(Приложение 2). Индекс насчитывался по 28 показателям, основные направления это: инфраструктура; степень развития онлайн расходов; вовлеченность государство, граждан и бизнеса в использование продуктов и возможностей цифровой экономики.

По Индексу цифровой экономики и общества, рассчитывающимся Европейской комиссией для семнадцати стран не входящих в ЕС, в 2018 году Россия заняла только 12 место из 17(Приложение 3). И наконец, по индексу IMD World Digital Competitiveness Ranking Россия на 2019 год занимает только 38 место(Приложение 4).

Большинство из приведенных индексов не отражают объективной картины. В совокупности мы можем сделать вывод о том, что цифровое развитие в России запаздывает на фоне общемирового показателя. С 2017 года не произошло сильного рывка в цифровом развитии страны, но определенную положительную тенденцию заметить можно.

Также важно будет сказать о разработке общероссийского рейтинга цифрового развития регионов. Инициатива исходила от от Совета Федерации. Подобные рейтинги появлялись и до этого в связи с актуализацией данной темы. В 2018 году бизнес школа «Сколково» подготовила рейтинг регионов по цифровизации. В целом показатели совпадали с основными проектами программы «Цифровая экономика Российской Федерации». В лидерах ожидаемо оказались Москва, Татарстан и Санкт-Петербург. Из неожиданных лидеров 4 место занял ХМАО, а 6 - ЯНАО. Десятку замыкали Ленинградская и Челябинская области (Приложение 5). Единый государственный рейтинг на сегодняшний день еще не реализован, на начало 2020 года Минкомсвязи только утвердила критерии, которые лягут в основу индекса. Рассмотрим основные направления деятельности России по цифровизации.

Направления цифрового развития были разработаю Экспертным советом при Правительстве РФ по цифровой экономике. Основные цели включают в себя:

1. Вовлеченность граждан и хозяйствующих субъектов в цифровом пространстве.
2. Создание необходимой инфраструктуры.
3. Создание необходимых цифровых экосистем для хозяйствующих субъектов.
4. снижение издержек при взаимодействии хозяйствующих субъектов, граждан и государства.
5. Повышение конкурентоспособности экономики за счет цифровых преобразований.[[17]](#footnote-17)

В Российской Федерации подход к цифровизации в целом заключен в экономическом секторе. Мотивация внедрения цифровых технологий, в первую очередь, экономическая. На национальный проект по данным 2019 года выделено около 1,6 трлн рублей, безусловно, проект являет очень масштабным и одним из приоритетных.

Национальный проект разделен на шесть федеральных проектов: Нормативное регулирование цифровой среды, Информационная инфраструктура, Информационная безопасность, Цифровое государственное управление, Цифровые технологии и Кадры для цифровой экономики.[[18]](#footnote-18) Нормативное регулирование включает в себя разработку необходимых правовых положений, которые обеспечили бы развитие цифровых технологий. Информационная инфраструктура включает в себя каналы связи, дата-центры, необходимость разработки соответствующего софта. Причем акцент делается на разработку отечественного ПО. Информационная безопасность отвечает за шифрование и безопасную передачу, хранение данных. Цифровое государственное управление - предоставление государственных услуг гражданам. Размытое «Цифровые технологии» отвечают за внедрение в России новейших технологий по типу искусственного интеллекта, машинного обучения, блокчейн, обработка больших данных и многого другого. Кадры для цифровой экономики отвечают за разработку программ подготовки с нуля узких специалистов для сфер цифрового развития, а так же переподготовку кадров связанных с цифровыми технологиями.

Как мы видим в «Цифровую экономику» входит практически все, от государственного управления и кадров до обеспечения национальной безопасности. Подобное смешение понятий часто приводит к путнице. Принятая из необходимости экономического роста национальная программа включает в себя самый широкий спектр различных направлений не связанных с экономикой напрямую. Соответственно и цели программы зачастую не совпадают полноценно с деятельностью исполнителей. Подобное разобщение может быть губительно для национальной стратегии, поскольку в государственном управлении совпадение целей и реальных результатов базовая составляющая.

Одной из наибольших проблем современной политики цифровизации является отсутствие необходимой законодательной базы. Внедрение новых законов, регулирующих те или иные правоотношения в сфере цифрового развития, один из первых шагов, которые необходимо сделать для успешного внедрения новых технологий. Старая нормативная база создавалась еще до появления даже разговоров о конкретных технологиях. Так например, блокчейн или искусственный интеллект на сегодняшний день не подпадают ни под один из действующих законов полноценно. Из 20 приоритетных правительственных законопроектов в сфере цифрового развития принят только один, закон о цифровых сделках.[[19]](#footnote-19) Множество проектов еще находится в доработке и даже не дошли до стадии рассмотрения. Примером такого законопроекта является закон о «регулятивных песочницах», по сути создающий инструмент для пилотной применения новейших технологий. Соответственно без наличия нормативного обоснования ни одна из прорывных инноваций не может быть реализована.

Также в рамках программы наблюдается отсутствие институциональной инфраструктуры. В последние два года положение дел улучшается, во множестве регионов создаются профильные комитеты, например, Комитет цифрового развития Ленинградской области или совсем новообразованное Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан. Однако эти регионы являются лидирующими в цифровом развитии, существует еще множество регионов, где отсутсвует необходимый орган для цифровизации, а соответственно данные регионы никак не могут реализовать план программы в полной мере.

Наблюдается разрыв в уровне развития технологий по различным отраслям. Наиболее прогрессивными отраслями является финансовый сектор. Банки стремительно цифровизируются, а главный банк в стране «Сбербанк» участвует во множестве межотраслевых программ по внедрению новейших цифровых технологий. Менее развиты отрасли связанные с сельским хозяйством или строительством. Хотя случаются исключение. Как например в Ленинградской области с попыткой внедрить блокчейн-алгоритмы для совершения сделок по недвижимости.[[20]](#footnote-20)

Периодически наблюдаются проблемы связанные с информационной безопасностью. Утречки персональных данных у различных компаний наблюдаются часто. Тесно связанной темой с информационной безопасностью является «суверенный интернет». Правительство крайне жестко готово охранять данные Россиян от иностранного вторжения, но при этом внутри России утечки повсеместны.

И наконец, одна из самых важных проблем это недостаток квалифицированных кадров. Причем как высшего, так и среднего образования. Для реализации национальной программы требуются сотни тысяч, если не миллионы кадров, которые пока негде взять на рынке труда.

Исходя из определения, данного в предыдущем параграфе, мы можем сделать вывод, что цифровизация в России находится в зачаточном состоянии. В российской государственном управлении цифровизация выступает только как попытка повысить эффективность уже существующих структур. Повышение безопасности - это второй критерий, на который опирается государственное управление в России. В России используется узкий подход к цифровизации. Хотя стоит так же отметить и следы широкого. Например, проект «Твой бюджет», он стал возможным благодаря цифровым технологиям. Но все же это не взаимодействие граждан друг с другом, а только с государством.

Согласно докладу о текущем развитии проектов в сфере цифровой экономики, подготовленный Аналитическим центром при Правительстве РФ в Ленинградской области на основе программы «Цифровое развитие Ленинградской области» в сфере цифровизации ведется работа по следующим направлениям:

* Оптимизация и повышение качества предоставления государственных и муниципальных услуг,
* повышение эффективности деятельности МФЦ,
* развитие ИТ,
* реализация на региональном уровне федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения,
* Развитие и обеспечение функционирования и безопасности инфраструктуры связи и обмена информацией,
* Развитие информационной инфраструктуры электронного правительства и обеспечение ее безопасности,
* Обеспечение безопасности ГИС,
* Развитие проектов «Умный регион», «Электронная госслужба».[[21]](#footnote-21)

На сегодняшний день осуществляется деятельность по всем направлениям. Особенный упор делается на создание и поддержание работоспособности информационной инфраструктуры органов государственной власти региона, обеспечение ее безопасности, а также поддержка сервисов электронного правительства. В ноябре 2019 года Губернатор Ленинградской области отметил, что развитие «Умных городов» является одним из наиболее амбициозных проектов в политике цифровизации региона.[[22]](#footnote-22)

Цифровизация в России, реализуемая в рамках «Цифровой экономики», запущенная в 2017 году является одним из приоритетных направлений сегодняшнего государственного управления. В рамках программы «Цифровой экономики» существует ряд отраслевых проектов, которые включают в себя самый широкий спектр отраслей цифровизации.

Намеченные планы реализации замедляются из-за ряда проблем: отсутствие необходимой законодательной базы, неразвитость институциональной инфраструктуры, , неоднородность внедрения цифровых технологий по отраслям, проблемы в обеспечении информационной безопасности, , недостаток квалифицированных кадров.

1.3 Основные доктрины информационной безопасности и политика цифровизации

Информационная безопасность Российской Федерации сегодня представляет собой список мер закрепленных в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы.

В России за реализацию информационной безопасности в рамках цифровизации отвечают множество государственных органов, наиболее важные из них - это Министерство цифрового развития, связи и массовых коммуникаций и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Защита информации в России подразделяется на три направления: защита информации от утечек, защита информации от несанкционированного воздействия, защита информации от непреднамеренного воздействия.

Утечка информации подразумевает под собой защиту от разглашения информации, от несанкционированного доступа и от доступа к информации разведкой. Защита от несанкционированного воздействия предотвращает доступ к информации субъекта, не имеющего разрешения. Субъектом могут быть отдельные физические лица, компании и государство. Защита от непреднамеренного воздействия предотвращает порчу информации пользователем или в силу каких-либо чрезвычайных ситуаций.

Обеспечение информационной безопасности является частью политики национальной безопасности. С этой стороны информационная безопасность в России рассматривается как список мер по защите национальных интересов в обычной логике национального суверенитета. Она выступает на равне с экономической, экологической, продовольственной и других составляющими национальной безопасности. Чаще всего в российском государственном управлении она рассматривается именно с этой стороны.

С другой стороны информационная безопасность является частью политики по развитию информационного общества. Под информационным обществом понимается общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.[[23]](#footnote-23) Соответственно, безопасность здесь будет выступать состоянием защищенности гражданина, общества и государства в условиях развития информационных технологий.

В Стратегии закреплено определение безопасности именно как защищенности гражданина, общества и государства. На наш взгляд, информационную безопасность мы можем рассматривать как взаимодействие не только государственных органов между собой, но и с обществом и отдельными гражданами. Управляемость в информационной безопасности заключается в первую очередь как охрана личных интересов граждан. Разумеется, охрана информационных ресурсов государственных структур тоже является частью интересов граждан. Но в современной России мы видим, что защищенность информации государства и защищенность интересов граждан расходятся и могут не совпадать. Одной из составляющих концепции управляемости является открытость или, в данном случае, свобода информации. В Стратегии закрепляется, что информационная безопасность является инструментом обеспечения конституционных прав и свобод граждан.

По Доктрине информационной безопасности, которая предшествовала Стратегии, выделяет следующие направления деятельности в рамках информационной безопасности:

* обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры.
* развитие в Российской Федерации отрасли информационных технологий и электронной промышленности.
* доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире.
* содействие формированию системы международной информационной безопасности, направленной в частности на защиту суверенитета Российской Федерации в информационном пространстве[[24]](#footnote-24).

Первые два пункта тесно пересекаются с направлениями «Цифровой экономики». В 2020 году когда мы говорим о информации и информационных технологиях, в первую очередь мы говорим о цифровизации и цифровых технологиях. Соответственно, обеспечение информационной безопасности в рамках политики цифровизации является приоритетным направлением.

Цифровизация дает широкие возможности к развитию информационного общества, но при этом острее становится вопрос об обеспечении безопасности. Реализация и развитие цифровой политики невозможна без должных мер контроля со стороны государства. Информационная безопасность должна обеспечить гармоничное внедрение и развитие цифровых технологий в России.

Не секрет, что новейшие технологии могут нести и угрозу частной жизни граждан и другим их конституционным правам. Например, сбор персональных данных, которые могут быть использованы в различного рода мошенничествах и преступлениях. Чтобы этого не допустить, в России развивают направление цифровизации, связанное с информационной безопасностью.

Идея «суверенного интернета» - прямое продолжение политики информационной безопасности. Закон о «суверенном интернете» вступил в силу 1 ноября 2019 года. Национализация интернета в России стала продолжением заботы государства о национальной безопасности. Причем с позиции российского государства мы не можем говорить о концепции управляемости, скорее сейчас закон рассматривается в рамках классического институционализма.

Термин «суверенный интернет» означает обеспечение технологической независимости российского сегмента Интернета.[[25]](#footnote-25) Под собой он подразумевает три направления: экономический протекционизм, связанный с цифровыми технологиями, обеспечение защиты национальной информационной инфраструктуры, а так же национальную организацию по использованию больших данных и их хранение на серверах, которые находятся на территории России. [[26]](#footnote-26)

Помимо международной политики, стоит рассмотреть информационную безопасность на местах. Региональные органы играют важную роль в обеспечении информационной безопасности. Местные органы государственной власти обеспечивают контроль над локальной информацией и информационной инфраструктурой. Соответственно функции местных органов схожи с федеральным аналогом. При этом зачастую наблюдается неравномерное обеспечение информационной безопасности на местах. Это происходит в силу следующих причин:

* Отсутствие кадров для осуществление необходимых функций в сфере безопасности.
* Недобросовестное отношение сотрудников к мерам по обеспечению информационной безопасности.
* Отсутствие необходимого бюджета для реализации всех мер по обеспечению информационной безопасности.
* Недостаточный уровень взаимодействия между органами по обеспечению безопасности информационной инфраструктуры, точек хранения информации и самой информации.

Помимо проблем, стоит сказать и о профильных комитетах в местных органах власти. Зачастую они связаны с комитетами по цифровому развитию. Так например, в Комитете цифрового развития Ленинградской области существует отдел информационной безопасности. В обязанности подразделения по обеспечению информационной безопасности относится мониторинг единой сети передачи данных, поиск возможных угроз и утечек. Кроме этого происходит мониторинг по охране незаконно использования персональных данных и документов исключительно внутреннего пользования. В Ленинградской области развитие информационной безопасности нацелено в первую очередь на охрану и защиту внутренних данных государственных структур.

Подводя итог, мы отметим, что основное направление развития информационной безопасности Российской Федерации закрепляется в Доктрине об информационной безопасности. Основными направлениями являются охрана данных от утечек, защита информации от непреднамеренного воздействия и от несанкционированного воздействия.

Развитие цифровизации и внедрение новейших коммуникационных технологий несут в себе угрозу информационной безопасности граждан, бизнеса и государства. Цифровизация и информационная безопасность тесно связаны, в современном подходе к государственному управлению информационная безопасность рассматривается уже как часть цифровизации, хотя защита информации возникла задолго до появления первого компьютера. Особенно актуальным становится предупреждение возможных угроз безопасности при внедрении цифровых технологий.

При подходе к пониманию места информационной безопасности в государственном управлении и концепции управляемости мы отметим его двоякость. Во-первых, информационная безопасность как часть национальной безопасности, то есть полностью подчинена вышестоящему направлению безопасности государства. Во-вторых, существует подход информационной безопасности в рамках информационного общества. Информационная безопасность как состояние защищенности гражданина, бизнеса и государства в условиях развития цифровых технологий. То есть информационная безопасность приобретает характер сотрудничества и взаимодействия акторов, будь то гражданин, компания или государство. Это открывает возможности для анализа информационной безопасности не просто как отрасли национальной безопасности, а как сферы сотрудничества заинтересованных сторон в обеспечение собственной защищенности.

Глава II Цифровизация и развитие кадрового потенциала в Ленинградской области: вызовы и перспективы

2.1 Основные потребности рынка труда и государственных органов в сфере цифровизации и информационной безопасности

Современные процессы цифровизации парадоксальным образом влияют на развитие социальных институтов, экономики и политики общества. А.А. Аузан в своем юбилейном докладе «Цифровая экономика: фактор человеческого капитала» в сентябре 2019 г. заявил о том, что цифровизация - это не исключительно процесс, связанный с техническим развитием, это процесс сокращения трансакционные издержек, сил «социального трения», которые катализируют появление и развитие новых социальных институтов. Важнейшей составляющей новых социальных институтов становится качество человеческого капитала. Новые институты формируют культурные и психологический черты человека, которые позволяют ему приобщаться к производству цифрового продукта и вступать в контакт с искусственным интеллектом. Развитие новый социальных институтов становится равным по важности техническому совершенствованию в рамках цифровизации. Человеческий капитал, главный ресурс развития социальных институтов, зачастую недооценивается, как финансовый или административный ресурсы. Для успешной политики цифровизации требуется достаточное внимание к проблемам обеспечения организаций и органов государственного управления соответствующим уровнем человеческого капитала.[[27]](#footnote-27)

Кадровая политика в современном государственном управлении все больше испытывает нехватку квалифицированных кадров в сфере цифровизации и информационной безопасности. Во всем мире спрос на специалистов в сфере информационной безопасности превышает предложение. Наличие необходимых кадров - базовая необходимость в любой сфере государственного управления.

Согласно исследованию Cybersecurity Workforce на 2019 год спрос почти в полтора раза превышает предложение на рынке труда в сфере информационной безопасности. В основе исследования лежал опрос 3237 специалистов в сфере кибербезопасности в различных сферах.( Приложение 6)

Так, например, Азиатско-Тихоокеанский регион испытывает дефицит в 2,6 млн человек в сфере кибербезопасности, в Европе существует потребность в дополнительных 291 тыс. человек.

По данным опроса нехватку специализированных кадров ощущают 65 процентов организаций. Среди опрошенных только 42 процента начинали свою карьеру с информационной безопасности, для других это не базовое направление. [[28]](#footnote-28)

В «Лабораторию Касперского» попадает, например, только один кандидат из сорока. Это зачастую связано с недостаточной компетенцией кадров. Больше всего требуется инженеров в сфере информационной безопасности, которые занимаются внедрением и развитием инфраструктуры информационной безопасности. Не хватает также и аналитиков, которые должны изучать произошедшие инциденты и предупреждать о возможных атаках. В России все большее количество работодателей сталкивается с проблемами информационной безопасности. [[29]](#footnote-29)

На сегодняшний день наибольший спрос на специалистов по информационной безопасности наблюдается в финансовых организациях и банках. Они оказываются наиболее подвержены кибератакам. Зачастую мы видим в СМИ новости об утечках персональных данных клиентов банков.[[30]](#footnote-30) Банкам приходится создавать целые отделы по информационной безопасности, поскольку все больше транзакций проводится с помощью цифровых технологий. Электронная коммерция оказывается наиболее уязвимой для новейших типов кибератак.

Следующими после финансовых компаний по спросу на специалистов информационной безопасности идут государственные структуры и сами компании, целенаправленно занимающиеся информационной безопасностью.

Сейчас наблюдается дефицит кадров, причем зачастую компаниям приходится переучивать выпускников университетов, потому что сфера информационной безопасности, да и IT в целом слишком стремительно меняется. Важнейшими качествами для специалистов в сфере информационной безопасности выдвигаются работа в команде и межотраслевая коммуникация.[[31]](#footnote-31) Подобные навыки логично вытекают из давней проблемы постановки технического задания программистам, связи бизнеса, публичной политики и конкретного цифрового продукта, который необходимо создать.

Кроме этого на рынке труда наблюдается потребность в консалтинге в сфере информационной безопасности и профессиональную экспертизу. Сейчас крайне актуальным становятся и смежные специалисты. То есть для которых информационная безопасность является субпрофессией. Скажем, например, экономист со знанием систем информационной безопасности будет крайне востребован на рынке труда.

В государственной службе еще несколько лет назад говорили о необходимости компьютеризации, обучения кадров работе с электронными системами. Сейчас наличие компьютеров и электронных систем передачи данных является данностью.

Цифровизация задает высокие темпы развития информационных технологий и государственного управления. Для того, чтобы управление оставалось эффективным необходимо постоянно повышать квалификацию кадров. Внедрение новейших цифровых технологий будет бесполезным, если органы государственного управления не будут их использовать по причине отсутствия квалификации.[[32]](#footnote-32)

Согласно ФЗ «О государственной гражданской службе Российской Федерации» государственные служащие обязаны на протяжении всего периода службы проходить профессиональную переподготовку и курсы повышения квалификации.[[33]](#footnote-33) Соотвественно сейчас множество курсов переподготовки государственных служащих связано с цифровыми умениями.[[34]](#footnote-34) За 2019 год более 13 тысяч государственных служащих прошли курсы повышения квалификации в Центре подготовки руководителей цифровой трансформации на базе РАНХиГС.

При принятии на государственную службу кандидат должен отвечать ряду критериев и обладать рядом навыков и знаний. Применительно к нашей теме существует три блока навыков в области ИКТ:

1. навыки работы с системами межведомственного взаимодействия и электронного документооборота;

2. умение работать с системами управления государственными информационными ресурсами;

3. навыки работы с информационно-аналитическими системами, обеспечивающими сбор, обработку, хранение и анализ данных;

4. умение работать с нормативно-правовыми информационными системами;

5. знание основ информационной безопасности в части использования персональных данных, хранения и обработки служебной информации, а также использования сети Интернет в служебных и персональных целях. [[35]](#footnote-35)

Основы информационной безопасности в современной государственной службе являются уже необходимым навыком. От государственных служащих требуют соблюдения требований по хранению и передаче информации.

Рассматривая рынок труда сферы информационной безопасности, стоит отмечать, что квалифицированные кадры необходимы не только в государственном управлении, они также необходимы подрядчикам, исполняющим государственный заказ по обеспечению безопасности информационной инфраструктуры. Кроме это различные компании также заинтересованы в развитии данного направления. Формируемые отделы информационной безопасности в компаниях, профильные компании по информационной безопасности и государственные органы информационной безопасности вместе создают единый рынок труда, который сейчас испытывает сильный дефицит кадров. Помимо инженеров, каждой из групп акторов необходимы кадры, которые не только будут разбираться в информационной безопасности, но также и готовы наладить коммуникацию с другими группами акторов. Государство нуждается в кадрах для связи с профильными компаниями и отделами внутри непрофильных компаний, так и другие группы нацелены на взаимодействие друг с другом.

В Ленинградской области к необходимым навыкам и знаниям для исполнения должностных обязанностей относятся различные компетенции в сфере цифрового технологий.[[36]](#footnote-36)

Среди необходимых навыков мы можем выделить работу с информационными системами электронного бухгалтерского учета «1С:Бухгалтерия», работу на компьютере с использованием OC Windows, MS Office, использование «Интернета», работа с информационного правовыми системами «Гарант», «КонсультантПлюс». Это достаточно общие навыки, которые уже много лет предъявляются при принятии на государственную службу. Рассмотрим, требования предъявляемые для профильной должности Правительства Ленинградской области в сфере цифрового развития.

Согласно конкурсным требованиям на должность Главного специалиста отдела стратегических проектов департамента развития цифровых технологий Комитета цифрового развития Ленинградской области приглашаются специалисты по направлению «Экономика и управление», «Электроника, радиотехника и системы связи», либо специальность или направление подготовки области образования «Гуманитарные науки», «Математические и естественные науки», либо направление подготовки «Информационная безопасность», либо специальность «Информационная безопасность автоматизированных систем», «Информационно-аналитические системы безопасности».(Приложение 7) Набор возможных специальностей чрезвычайно широк, потенциальный кандидат может обладать как специальностью в сфере управления, так и сугубо профильной «Информационная безопасность». Специалист также должен обладать знанием законов о «Персональных данных», «Об информации, информационных технологиях и о защите информации», « О стратегическом планировании Ленинградской области», « О Концепции социально-экономического развития Ленинградской области на период до 2025 года», основные положения законодательства об электронной подписи, «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

В Ленинградской области наблюдается тенденция к привлечению кадров в сферу цифрового развития из самого широкого круга специальностей. К кандидату выдвигаются требования не только узконаправленного характера, как знание информационных систем и структур, но также управленческие навыки, стратегическое мышление.

Отдельно стоит выделить требования к умению работать в информационных системах комитета, в том числе прикладных системах взаимодействия с гражданами и организациями. Подобное требование говорит о том, что Правительство Ленинградской области заинтересовано не в закрытости процесса цифрового развития, а в открытой и прозрачной коммуникации, взаимодействию и сотрудничеству с гражданами и бизнесом в цифровом развитии.

В России наблюдается нехватка человеческого капитала для обеспечения намеченных темпов цифровизации. Рассмотренная кадровая политика в сфере цифрового развития и информационной безопасности показывает, что цифровой рынок труда испытывает большой спрос на специалистов в мире. В России также наблюдается спрос как на инженеров в сфере информационной безопасности, так и на аналитиков. Основной спрос на спецалистов в сфере информационной безопасности формирует банковский сектор, государственные органы, а также компании занимающиеся обеспечением информационной безопасности.

В сфере цифрового развития наблюдается потребность в кадрах способных стать связующим звеном между глобальной стратегией и конечным исполнителем. Среди необходимых навыков - работа в команде и коммуникация между исполнителями. В государственной службе цифровизация задает тренд к введению новых стандартов государственного служащего, среди них: навыки работы с электронным документооборотом, умение пользоваться информационными системами различного толка, базовые знания в сфере информационной безопасности.

Ленинградская область в соответствии с федеральным уровнем следует тренду внедрения цифровых навыков в государственном управлении. Помимо продвинутого использования компьютера и информационных систем, профильные специалисты должны разбираться в стратегическом плане развития направления цифровых технологий и региона. Также в государственном управлении как и в частном секторе необходимым навыком становится коммуникация, работа в команде и другие различные виды взаимодействия с другими государственными структурами, гражданами и бизнесом.

Перед нами встает вполне логичный вопрос, как возможно пополнить человеческих капитал. Одним из основных способов производства человеческого капитала является образование, а конкретно высшая школа.

2.2 Развитие рынка образовательных программ в сфере цифровизации и информационной безопасности.

Образование выступает в качестве основного производителя человеческого капитала. В упомянутом в предыдущем параграфе докладе А.А. Аузана о человеческом факторе в цифровизации отмечается, что современное образование создает парадоксальную ситуацию противостояния естественного интеллекта, человеческого капитала, и искусственного интеллекта, продукта цифровизации. Современные образовательные программы подрывают положение человека перед искусственным интеллектом, что создает большую угрозу назначению всего человеческого капитала. Основной задачей образовательных программ должно выступать формирование необходимых умений для взаимодействия человека с искусственным интеллектом и алгоритмами цифрового развития, но при этом нельзя ставить естественный интеллект в подчиненное положение перед искусственным.[[37]](#footnote-37)

Дефицит кадров в сфере информационной безопасности и цифрового развития может быть решен только с помощью формирования необходимой системы подготовки кадров в высшей школе. Ведущие университеты России уже сегодня обучают по соответствующим направлениям студентов, рассмотрим каким компетенциям и навыкам обучают студентов в высшей школе.

Согласно Стратегии социально-экономического развития Ленинградской области до 2030 года одним из приоритетов развития Ленинградской области является развитие ИКТ. Одним из направлений данной стратегии является кадровое обеспечение сферы ИКТ в Ленинградской области.

Ленинградская область, являясь одним из лидеров цифрового развития регионов России, заинтересована в расширении кадровой подготовки по данному направлению.[[38]](#footnote-38) Одним из дополнительных пунктов Стратегии ставится необходимость создания рекрутингового и консалтингового центра « Профессия в IT». Центр потенциально может стать связующим звеном на рынке труда.

Основной базой рекрутинга кадров для сферы информационной безопасности могут стать ВУЗы Санкт-Петербурга. По соответствующим направлениям проводят подготовку в основном два ВУЗа - это ИТМО и Политех.

Магистерская программа в ИТМО «Информационная безопасность» реализуется на базе факультета безопасности информационных технологий. (Приложение 8) Программа предполагает следующие специализации:

* + Технологии обеспечения кибербезопасности
  + Управление информационной безопасностью
  + Аналитика информационной безопасности
  + Информационная безопасность компьютерных систем
  + Криптографические методы защиты информации
  + Кибербезопасность в банковской сфере
  + Информационная безопасность специализированных систем

Данная программа готовит узких специалистов в сфере информационной безопасности. Выпускник в конце обучения сможет претендовать на должность инженера-разработчика в сфере информационной безопасности. Кроме этого в программе курса отдельным пунктом выделяется специализация кибербезопасности в банковской сфере. Как мы говорили в предыдущем параграфе банковский сектор создает основной спрос на специалистов информационной безопасности. Еще одной сильной стороной курса является наличие программ по креативным технологиям и эмоциональному интеллекту. Среди важнейших качеств на рынке труда выделяется коммуникация и работа в команде.

Другая магистерская программа, осуществляющая подготовку в данной сфере, «Математические методы компьютерной безопасности» на базе Института прикладной математики и механики Политеха. В рамках данной программы профильные дисциплины схожи с программами ИТМО, выделяется только специализация по «Специальным разделам математики». В Политехе больше делают упор на теоретическую часть, когда как в ИТМО на практическую. (Приложение 9)

Приведенные программы готовят узких специалистов в сфере информационной безопасности. На рынке труда необходимы не только кадры узкой специальности, но и кадры для которых информационная безопасность не единственная специализация. Для государственной службы помимо того, что работник разбирается в информационной безопасности, необходимо чтобы он понимал общую стратегию государственной политики, понимал нормативно-правовую базу информационной безопасности и цифровизации.

Реализация государственных программ нуждается также в специалистах, которые могут обеспечить связь между глобальными стратегическими проектами и конкретным техническим заданием для узкопрофильного специалиста. Подобные кадры для государственной службы готовятся в ведущих университетах России.

Среди российских программ подготовки управляющих кадров для политики цифровизации и информационной безопасности можно выделить магистерские программы в Ранхигс и ВШЭ.

В рамках магистратуры Государственного и муниципального управления существует программа «Цифровое государство (стратегическое развитие информационного общества)». Программа напрямую не связана с информационной безопасностью, но она обучает управленцев в сфере цифрового развития. То есть, она подготавливает специалистов, которые становятся связующим звеном между глобальной стратегией и внедряемой цифровой технологией. Одним из акцентов программы является формирование практических умений и управленческих навыков администрирования цифровых и информационно-коммуникационными технологий в государственном и частном секторах. (Приложение 10) Подобные навыки оказываются крайне полезны в условиях, когда государство, бизнес и граждане рассматриваются через призму сотрудничества, или, проще говоря, через призму концепции управляемости. Программа позволяет сочетать навыки управления и знания цифровых платформ, возможностей, которые они дают. В данном случае, это ключевые кадры для государственной службы при проведении политики цифровизации.

Стоит отметить программу ВШЭ «Управление информационной безопасностью». К компетенциям выпускников в ней относят сетевую безопасность, защиту критически важных инфраструктур, архитектуру компьютеров и сетей.(Приложение 11) Программа позволяет студенту приобрести не только сугубо узкие знания в сфере информационной безопасности, но также ианалитические и прогностические умения в сфере безопасности и цифровизации. Программа подготавливает менеджмент в сфере информационной безопасности. Это потенциально интересно для государственной службы тем, что в условиях менеджериальной модели государственного управления, к которой сейчас стремится Россия, обеспечение информационной безопасности как товара на рынке услуг, кажется крайне актуальным.

Стоит отметить и актуальные для Ленинградской области направления в СПбГУ. Первая магистерская программа связана с государственной службой скорее косвенно. «Управление бизнесом в цифровой экономике» как и предыдущая программа обучает в первую очередь менеджеров в сфере цифровизации. (Приложение 12) Программа делает акцент на экономические процессы в политике цифровизации. Дисциплины дают необходимую общую базу цифровых процессов, как «Информационная безопасность» и «Цифровая экономика: современные вызовы»., при этом программа делает упор на бизнес-аналитике и аналитике финансов. Программа потенциально позволяет создать кадры, которые будут понимать как развивается экономика в цифровом мире, взаимоотношения государства и бизнеса в цифровых инновациях.

Наконец, программа «Цифровое публичное управление» обучает кадры для публичной политики и сферы цифровизации. (Приложение 13) Она подготавливает управленческие кадры цифровизации, от менеджмента она отличается тем, что выпускники данной программы имеют необходимые компетенции и понимание взаимодействия государства, бизнеса и гражданского общества в принятии решения. Большинство дисциплин направлено на новейшие сферы управления, создаваемые цифровыми технологиями, «Открытое правительство: сравнительный анализ», «Инициативное гражданское бюджетирование: онлайн платформы», «Умное управление городами» все эти дисциплины обучают студентов не столько повышению эффективности цифровизации, сколько расширению применения цифровизации в политике и принятии решений.

Сравним, наконец, какие же основные компетенции выделяются в программах по подготовке управленцев в сфере цифровизации и специалистов в сфере информационной безопасности.

Программы информационной безопасности сравнительно не новые, вновь они актуализировались в период цифровизации бизнеса и государства. Появились новые угрозы связанные с киберпреступностью, новейшие программы подготовки специалистов стали ответом на новейшие технологии применяемые мошенниками. Во всех проанализированных программах акцент делается на технологическом обеспечении информационной безопасности, обеспечении безопасности компьютерных сетей. Явно наметилась тенденция к расширению пула от узкоспециализированного направления к междисциплинарности. Помимо сугубо технических умений, в программы университетов добавляют курсы по менеджменту, координации, работе в команде. Современные российские университеты все больше отходят от узкоспециализированных направлений, выпускники после университета помимо hard skills приобретают и soft skills. Второе относится к коммуникации работников между собой. Это безусловно является ответом на спрос на рынке труда, где командная работа и коммуникация в коллективе зачастую имеют доминирующую позицию. Университеты стремятся дать техническую базу и при этом увязать их с коммуникативными умениями, которые так востребованы. Для подготовки управленческих кадров в политике цифровизации также характерна междисциплинарность и многофункциональность. Направление менеджмента в цифровой политике стало актуальным после 2017 года и соответствующего указа президента. В первую очередь рынок труда был сформирован государственной службой. И на сегодняшний день менеджеры в сфере цифрового управления и регулирования в первую очередь востребованы на госслужбе. Поскольку специфика работы предполагает формирование для исполнителя четкого алгоритма действий, плана и ожидаемых результатов. Управленческие программы в сфере цифровизации формируют взгляд выпускника на политику цифровизации как на совокупность взаимодействующих между собой акторов бизнеса, государственных структур и гражданского общества.

Данные программы прививают выпускникам умения, с помощью которых они могут стать тем самым связующим звеном между непосредственно исполнителями и общей стратегией. Специалист-выпускник управленческих программ в сфере цифрового развития может связать инженера по информационной безопасности и Стратегию развития информационного общества в России.

В Ленинградской области управленческие кадры могут быть необходимы при реализации региональной программы «Цифровое развитие Ленинградской области», специалисты с техническим базисом и управленческими навыками могут претворить в жизнь общую стратегию цифрового развития региона в реальных технических заданиях для подрядчиков в сфере информационной безопасности или цифрового развития.

Подводя итог, высшая школа в России в сфере цифровизации еще только развивается, имеется ограниченный набор программ, осуществляющий подготовку управленцев в сфере цифрового развития и информационной безопасности. Государственные структуры заинтересованы в том, чтобы выпускники университетов не только знали как работают технологии, инфраструктура, но и умели принимать управленческие решения, формировать долгосрочный план развития.

На основе рассмотренных программ мы можем сделать вывод о том, что Правительству Ленинградской области в лице Комитета цифрового развития стоит обратиться к прямому взаимодействию с ВУЗами для корректировки образовательных программ. Существующая проблема недостаточной квалификации выпускников после обучения в ВУЗах может быть решена с помощью налаживания тесного сотрудничества между Комитетом и конкретными бакалаврскими и магистерскими программами в ВУЗах Санкт-Петербурга. Комитет может таким образом отслеживать потенциальных кандидатов с начала их обучения, а также вносить предложения по корректировке образовательных программ в соответствии с задачами, стоящими перед ОГВ и Правительством Ленинградкой области. Такое взаимодействие будет выгодным и для студентов, которым будет дана возможность получить больше практики реальной работы и понимания целей и задач, стоящих перед Правительством Ленинградской области, и ОГВ – в целом, в контексте цифровизации систем управления.

Современная российская высшая школа трансформируется от узконаправленного прививания умений, необходимых для развития искусственного интеллекта, к более широкому - поддержке творческого и командного потенциала человека. Данный сплав из творческого мышления, работы в команде и технических умений должен стать основой для развития человеческого капитала в России. Университеты стараются в свою очередь развивать программу подготовки в соответствии с потребностями рынка труда. Университеты постепенно вводят в образовательные программы курсы по soft skills, т.е. прививают будущим специалистам корпоративную культуру, коммуникативные навыки и навыки работы в команде.

Глава III Опыт реализации политики информационной безопасности в Ленинградской области

3.1 Проект «Территория Безопасности» как пример общественной иниицативы в сфере информационной безопасности

Понятие национальной безопасности включает в себя множество аспектов. В соответствии с концепцией  governance, о которой мы говорили в 1 главе, безопасность может пониматься как safety и как security. Появление подобного разделения является логичным продолжением идеи о политике как о платформе взаимодействия государства и гражданского общества в принятии решений. Security выступает как безопасность государства, государственного суверенитета и государственных органов. Safety понимается как безопасность личности, отдельно взятого человека.[[39]](#footnote-39) Зачастую в России наблюдается смешение данных понятий, подмена одного другим.

В условиях цифровой трансформации общество столкнулось с новейшими вызовами в сфере безопасности. Нарастающие процессы информатизации, основанные на развитии технологий, поставили под угрозу связанные с ними экономические и правовые аспекты использования интеллектуальной собственности как бизнеса, так и частных лиц. Особым объектом все больше рассматривается - психический мир личности, который находится под прессом эпохи постправды, новых видов СМИ, социальных сетей.[[40]](#footnote-40) Цифровое развитие общества обострило противоречие в подходах к обеспечению информационной безопасности, с одной стороны это структурная безопасность государства, а с другой безопасность личности и его психики.

Понятие информационной безопасности разнится в зависимости от сферы и целей, в которых используется. Кибербезопасность - это сравнительно новое понятие, которое также относится к информационной безопасности, но подразумевает под собой защиту данных в условиях современных цифровых коммуникаций или по-другому в киберпространстве.[[41]](#footnote-41)

Одной из важнейших составляющих процесса осуществления национальной безопасности является работа с гражданами, разработка методик обучения основам безопасности широких слоев общества.[[42]](#footnote-42) Обучающих программ в сфере информационной безопасности не так много, большинство из них нацелено на специалистов и менеджеров в данной сфере, но никак не на население.

В Ленинградской области нам представлен уникальный кейс многоаспектного развития проблематики информационной безопасности. С одно стороны, как security, с другой как safety. В данном параграфе мы рассмотрим проект, делающий акцент на психологической информационной безопасности отдельной личности, а в следующем на информационной безопасности структуры государства.

В Ленинградской области реализуется проект по популяризации и образовательной деятельности в сфере информационной безопасности «Территория БезОпасности». Проект реализуется на территории Ленинградской области с 2017 года. «Территория БезОпасности» (далее ТБ) разработан «Центром молодежных инициатив» совместно с «Центром студенческих инициатив «Северо-Запад».[[43]](#footnote-43)

Данный социальный проект реализуется на основе гранта Губернатора Ленинградской области при поддержке Комитета по печати и связи с общественностью. Также поддержку проекту согласно открытой информации оказали Комитет правопорядка и безопасности Ленинградской области, Общественная палата Ленинградской области, Законодательное собрание Ленинградской области.

Целью проекта создатели считают формирование и популяризацию принципов безопасного информационного пространства среди молодёжи и взрослого населения. Задачи проекта: профилактика социально-опасных форм поведения граждан, осуществление просветительной работы с населением в сфере кибербезопасности и методов профилактики негативных социальных явлений, обучение взрослого населения основам медиаграмотности.

Цель проекта выглядит логичной и востребованной, умение безопасного использования информационного пространства одно из базовых для человека, живущего в цифровую эпоху[[44]](#footnote-44). С задачами проекта все не на столько очевидно. В двух из трех выдвинутых задач упоминается профилактика негативного социального поведения граждан. Соответственно, мы можем сделать вывод о том, что для создателей проекта использование информационного пространства в первую очередь связано с угрозой негативного поведения личности. Но также стоит и отметить, что третья задача выделяется как обучение медиаграмотности взрослого, что с негативным поведением никак не связано. То есть, профилактика угроз проводится исключительно среди молодежи, но не среди взрослого населения.

С момента запуска проекта количество участников составило около 11 тысяч человек, в которых две трети составляют молодежь, 11 процентов родители и 17 процентов педагоги и специалисты по молодежной политике. Как отмечают сами руководители проекта, охват обучающих мероприятий проекта пока слишком мал.

Согласно мнению руководителей проекта проект поддерживают ряд лиц. Среди них мы отметим Драчева В. П., депутата Государственной Думы РФ, Пуляевского Д. В, заместителя председателя Законодательного собрания Ленинградской области, Сунгуров И. В. исполнительного директора Союза городов воинской славы, Пелина А., протоиерея отдела по взаимоотношениям Церкви и общества Санкт-Петербургской епархии. Исходя из отмеченных лиц, поддержавших проект, мы можем сделать вывод о том, что он является частью публичной политики Ленинградской области и РФ в целом. Авторы проекта называют свой проект социальным, поддержка политических лиц и лидеров мнений делает его составляющей частью публичного политики. О характере образовательного контента может также говорить и поддержка Союза городов воинской славы. О развитии проекта также высказываются многие политические деятели от муниципальных депутатов до председателя Общественной палаты Ленинградской области.

Одним из основных направлений деятельности участников проекта стала «Азбука кибербезопасности». В Азбуке представлены методические рекомендации по проведению занятий с подростками. В азбуке, например, приведено такое определение кибербезопасности - это условия защищенности от физических, психологических или других типов воздействий распространяемых посредством киберсреды, в которой человек еще не выработал правил поведения. Авторы выделяют два аспекта: социальный и технический, то есть, защиту от негативного информационного воздействия и защиту объектов информационной инфраструктуры от кибератак.[[45]](#footnote-45) В примечании приводится ссылка на Доктрину информационной безопасности РФ от 2016 года. Любопытно, рассмотреть и определение понятия контентная война. Контентная война в Азбуке - это элемент кибервойны, направленный на интеллектуальное поражение как отдельной личности так и народа в совокупности. Процесс контентной войны характеризуется комплексом информационно-психологических операций, осуществляемых через киберпространство с целью воздействия на психику и поведение представителей потенциального противника. В примечании приводится ссылка на Устав армии США от 1987 года, а так же на работу Ольшанского Д.В. «Основы политической психологии» 2001 года. Определение взято из материалов двадцати и тридцати летней давности, в момент когда еще не существовало ни Web 2.0, ни «Интернета вещей».

Другим важным направлением проекта является разработка профилактических фильмов: «Территория БезОпасности», « Отцы и дети. Территория БезОпасности», «Общественная грамотность в киберсреде». В совокупности в фильмах участники проекта рассказывают свое видение на киберагрессию, гибридных войнах, угрозы погружения молодежи в интернет-пространство, «сетевые революции».

В последнем фильме проекта «Общественная грамотность в киберсреде» рассматриваются «сетевые революции». В фильме приводится пример протеста «желтых жилетов» во Франции, как массу протестующих, организованную и подталкиваемую «третьим лицом» с помощью информационных ресурсов. Также под «третьими лицами» понимаются специалисты из центров кибербезопасности США и других западных стран, которые намеренно создают провоцирующий контент. Также в фильме отмечается инфантилизм современной молодежи из-за «деградационного контента» в Интернете и по ТВ, который в свою очередь провоцирует молодежь на протестное поведение.

Как отмечается в описании к фильму авторы предлагают принципы защиты от информационно-алгоритмических атак. В первую очередь они настаивают на том, что совместными усилиями власти и общества необходимо выстроить систему информационного противостояния провокациям и на основе реальных дел формулировать в интернете и в оффлайн свою информационную повестку. Под провокациями в фильме понимается расшатывание положения действующих властных лиц.

Еще одним направлением проекта являются образовательные мероприятия в Ленинградской области. В программе мероприятий запланирован просмотр фильма, о котором говорилось выше, а также тренинг «Защита здоровья в киберсреде». Встречи проводятся в каждом из районов Ленинградской области. Встречи реализуются на базе образовательных учреждений районов и нацелены большей частью на школьников.

Продолжением образовательных мероприятий стал конкурс «Ленинградская область – Земля Героев», на котором присутствовали Председатель общественной палаты Ленинградской области Трусов Ю.В., Первый заместитель председателя Комитета правопорядка и безопасности Рябцев В. Б.и начальник отдела социальных коммуникаций Комитета по печати и связям с общественностью Ленинградской областиЗеленин А.А.

Присутствие на подобном конкурсе представителей руководства региона означает интерес к подобной тематике со стороны власти. Причем нельзя не отметить, что организаторы проекта смешивают патриотическое воспитание с основами кибербезопасности.

Основным направлением деятельности всего проекта является не только и не столько просвещение в сфере информационных пространств и личной безопасности в сети, сколько патриотическое воспитание молодежи. Во всех представленных направлениях проекта четко прослеживается стремление к прививанию молодежи ценностей, основанных на исторической памяти Великой Отечественной войны, поддержка существующего режима в России. Угрозами же в данном проекте представлены протестное поведение, поддержка западных ценностей в противовес официальному взгляду России.

С подобными акцентами вполне логичным оказывается поддержка проекта со стороны руководителей региона, общественных организаций, связанных с прославлением победы в Великой Отечественной войне. Подобное идеологическое направление или национальная идея уже много лет разрабатывается федеральным правительством.[[46]](#footnote-46) Упоминание ВОВ в новогоднем обращении Президента и других его речах задает определенный тренд, который распространяется и на региональные власти.

Данный проект представляет собой альтернативный взгляд на информационную безопасность в России, если до этого мы говорили о технологической безопасности, внедрении цифровых технологий в общественные институты и взаимодействие граждан с помощью них, то здесь информационная безопасность понимается как способность государства создать повестку дня и его культурно-историческое обоснование для сохранения существующего режима. Данный проект является попыткой укрепить позиции официальной точки зрения государства на политику, историю и культуру в условиях всеобщей информатизации и цифровизации.

Проект «Территория БезОпасности», реализуемый на территории Ленинградской области, в заявленной цели стремится к развитию кибербезопасности региона, а также повышению сознательности граждан в данной сфере. Проект курируется «Центром молодежных инициатив» совместно с «Центром студенческих инициатив «Северо-Запад», что примечательно проект поддержан грантом Губернатора Ленинградской области, что говорит о том, что региональные власти заинтересованы в развитии подобного направления и считают его перспективным.

Проект получил широкую поддержку не только от Комитета по печати и связей с общественностью, но также Комитета правопорядка и безопасности и Общественной палаты Ленинградской области. Федеральным партнером проекта является Союз городов воинской славы, который на прямую не связан с информационной безопасностью, поскольку имеет другую тематику.

В деятельность проекта входит создание просветительских фильмов, методических рекомендаций «Азбуки кибербезопасности», а также мероприятия по просвещению молодежи в сфере кибербезопасности. Руководители проекта заявляют о том, что проект развивает социальное направление кибербезопасности, воспитывает в молодежи нравственные ценности, которые помогают бороться с «психологическими атаками» из вне. На деле же проект основан на патриотическом воспитании с привязкой к цифровой эпохе, внутри проекта открыто критикуется протестное поведение, отстаивается существующий режим и его историко-культурные ориентиры. Данный подход может стать альтернативным взглядом к рассматриваемой проблематики политики информационной безопасности Ленинградской области.

3.2 Работа государственных органов по обеспечению информационной безопасности в Ленинградской области

Сфера информационной безопасности все больше становится заметной в публичной политике. В предыдущем параграфе мы рассмотрели проект, который поддержала Ленинградская область в сфере информационной безопасности. Проект развивает идею информационной безопасности, как сохранение культурных ценностей в повсеместной цифровизации общества. Существует и другой подход, согласно нему информационная безопасность является площадкой сотрудничества государства, граждан и частного сектора по обеспечению безопасности инфраструктуры и информационных потоков.

Регулированием сферы информационной безопасности, разумеется, занимаются профильные государственные институты. В России государственные органы являются системообразующими в формировании информационной защищенности общества.

В Ленинградской области подобным органом является Комитет цифрового развития. Комитет осуществляет регулирующую функцию в политике цифровизации в Ленинградской области, при этом, разумеется, на него положены и задачи по обеспечению информационной безопасности населения региона. (Приложение 14) В полномочия Комитета в сфере информационной безопасности входит:

* организация и осуществление защиты информации, содержащейся в государственных информационных системах региона;
* методическое и техническое обеспечение по вопросам защиты персональных данных в органах исполнительной власти региона, органах местного самоуправления и в подведомственных им учреждениях;
* обеспечение безопасности значимых объектов критической информационной инфраструктуры. [[47]](#footnote-47)

Таким образом, к функциям комитета в сфере информационной безопасности относится в первую очередь охрана информации и каналов коммуникации внутри государственных органов.

Меры по обеспечению информационной безопасности осуществляются с помощью взаимодействия Комитета как регулятора и частных компаний как исполнителей. Комитетом заключаются контракты на техническое обеспечение защиты информации. Существует ряд компаний предоставляющих Комитету технические возможности по мониторингу, выявлению угроз и обеспечению защищенности информационной инфраструктуры региона.

Positive Technologies - это российская компания, занимающаяся созданием систем анализа защищенности и соответствия стандартам. Комитет цифрового развития Ленинградской области использует продукт компании MaxPatrol SIEM, который позволяет осуществлять мониторинг всей IT-инфраструктуры и выявлять инциденты информационной безопасности.[[48]](#footnote-48)

Комитет использует продукт компании для мониторинга единой сети передачи данных Правительства Ленинградской области, отслеживание состояние всех устройств подключенных к внутренней сети, выявление возможных угроз при передаче данных.

Positive Technologies - это одна из крупнейших компаний в России в сфере информационной безопасности. Компания существует уже около 15 лет, ее большим преимуществом помимо самого продукта и его качества, безусловно является лицензия Федеральной службы по техническому и экспертному контролю на разработку средств защиты конфиденциальной информации, лицензия ФСБ на работу со средствами криптозащиты и оказание услуг в области государственной тайны, и наконец, лицензия Министерства обороны РФ в создании средств защиты информации. Подобные лицензии открывают доступ на рынок заказов государственных органов и компаний и являются более весомым фактором для сотрудничества, чем удобность, доступность и цена.

Значимость компании на рынке можно определить по партнерам, с которыми она работает. Продукты Positive Technologies использует не только Комитет цифрового развития Ленинградской области, но также Министерства обороны, иностранных дел, финансов РФ, Федеральная налоговая служба, Правительство Москвы. Причем, интересно, что продукты компании почти не используются в региональных профильных органах, за исключением Москвы, Санкт-Петербурга и Ленинградской области.

Следующей компанией, с которой сотрудничает Комитет цифрового развития является Инфотекс. Инфотекс также является российской компанией по разработке программно аппаратных средств защиты информации.[[49]](#footnote-49) Компания входит в топ-5 крупнейших компаний в сфере защиты информации.(Приложение 15) Если Positive Technologies создает инструменты для мониторинга системы, то Инфотекс создает защищенные каналы передачи данных. Инфотекс занимается разработкой сервисов информационной безопасности, создает инфраструктуру информационной безопасности.

Комитет цифрового развития покупает у Инфотекса технологию VipNet. Данный продукт позволяет создать программно-аппаратную систему передачи данных. В Ленинградской области Комитет является связующим звеном между органами власти региона, которым необходимы защищенные каналы передачи данных, и Инфотексом, которая предоставляет необходимую инфраструктуру для этого.

Инфотекс имеет сертификацию ФСБ и ФСТЭК. Одним из ее главных преимуществ является сертификация по международному стандарту. Компания сотрудничает с Microsoft и Samsung. Компания также осуществляет международную деятельность. Инфотекс выигрывает не только как отечественный разработчик, получивший лицензию от структур, обеспечивающих государственную безопасность, но и как партнер международных компаний.

Компанией осуществляющей защиту единой сети передачи данных Ленинградской области от утечек корпоративных данных является Группа компаний InfoWatch. Для Комитета цифрового развития InfoWatch в 2019 году начал предоставлять программное обеспечение по мониторингу корпоративных данных. InfoWatch осуществляет анализ потенциальных утечек в массиве данных внутренней сети Правительства Ленинградской области, речь идет о персональных данных и служебных документах, не подлежащих публичному разглашению.

ГК InfoWatch быстро растущая компания, осуществляющая свою деятельность как в России, так и в мире. Компания в отличие от предыдущих партнеров Комитета работает на рынках Западной Европы, Ближнего Востока, Индии и Юго-Восточной Азии.[[50]](#footnote-50) Компания открывает представительства полного цикла по всему миру, например в Дубае и Куала-Лумпуре.

InfoWatch основана Натальей Касперской, одним из учредителей крупнейшей компании по обеспечению информационной безопасности в России «Лаборатории Касперского». По сути InfoWatch выросла из внутреннего проекта «Лаборатории Касперского». Компания также имеет лицензии ФСБ, ФСТЭК и Министерства обороны РФ на осуществление деятельности в сфере информационной безопасности. Компания оказывается тесно связанной с «Лабораторией Касперского», этим можно объяснить ее стремительный рост и выход на международные и региональные рынки.

Комитет цифрового развития использует продукт InfoWatch Traffic Monitor. Если предыдущие продукты позволяют следить за инфраструктурой и передачей данных, то продукт InfoWatch используется для отслеживания содержимого в передаваемых данных. Поскольку компания нацелена на предоставление услуг полного цикла, мы можем предположить, что Комитет в будущем будет использовать и другие продукты компании. InfoWatch используется Комитетом в первую очередь для выполнения задачи по охране персональных данных пользователей сети, граждан.

Помимо взаимодействия с различными частными компаниями Комитет цифрового развития тесно взаимодействует с другими органами государственной власти Ленинградской области и федерального правительства.

Поскольку одной из задач Комитета является поддержка единой сети передачи данных, обеспечение информационной безопасности при передаче данных, он разрабатывает методические требования к деятельности других комитетов в сфере цифрового обеспечения и безопасности обмена информацией.

Комитет отслеживает потенциальные угрозы внутри правительственной сети и уведомляет о потенциальных угрозах пользователей сети. Особенно стоит отметить работу по сохранению персональных данных пользователей. Комитет осуществляет взаимодействие с другими комитетами и подведомственными учреждениями рамках политики по обеспечению неразглашения персональных данных граждан.

Деятельность Комитета не так заметна в публичном поле, как например, реализация социальных проектов по гражданско-патриотическому воспитанию в цифровой среде, но при этом она является частью масштабной федеральной повестки, связанной с государственным управлением. О правильном воспитании и защите детей и подростков в цифровой среде ведется множество обсуждений в информационном поле, а о развитии и совершенствовании информационной безопасности меньше. Тем не менее, деятельность Комитета цифрового развития Ленинградской области в сфере защиты информации является частью публичной политики, поскольку основана на взаимодействии государственных органов с частным сектором и гражданами.

На примере Комитета цифрового развития Ленинградской области мы видим пример успешного осуществления государственной политики по обеспечению информационной безопасности. Комитет осуществляет широкое взаимодействие с государственными органами, подведомственными учреждениями, сторонними организациями.

Департамент информационной безопасности и инфраструктуры обеспечивает безопасность Единой сети передачи данных Ленинградской области. Еще одной сильной чертой Комитета в данном направлении является успешное сотрудничество с частным сектором, компаниями, разрабатывающими ПО в сфере информационной безопасности. Комитет сотрудничает с компаниями, входящими в топ-5 крупнейших компаний в сфере информационной безопасности в России.

При этом можно отметить, что Комитет не полностью использует имеющийся внутренний ресурс региона в лице молодых специалистов. В рамках деятельности Комитета проводятся мероприятия по повышению «цифровой» грамотности подростков, но не заметна в публичном пространстве работа с молодежью, которая может стать ценным источником кадров, о котором мы говорили ранее. Комитет может привлекать молодых специалистов в данной сфере с помощью организации ряда мероприятий в виде круглых столов, кейс-чемпионатов, что позволит не только рассмотреть потенциальных сотрудников, но и популяризировать деятельность всего Комитета.

Комитет цифрового развития, являясь одним из самых передовых в Правительстве Ленинградской области, на наш взгляд, недостаточное внимание уделяет продвижению и развитию имиджа Комитета в публичном пространстве. Так, например, в освещении социального проекта «Территория безопасности», который мы рассмотрели, совсем отсутствует упоминание о Комитете цифрового развития, хотя информационная безопасность или кибербезопасность является прямой задачей Комитета. Комитет мало заметен в общественной сфере и поддержке социальных проектов и инициатив населения. Помимо информационной безопасности существует еще множество направлений деятельности Комитета, о которых можно было бы рассказать в публичном пространстве.

Формирование положительного имиджа организации, государственного органа, на наш взгляд, является одним из самых важных в условиях нового менеджмента и концепции governance. Государственные органы, выступающие как часть рынка услуг, как партнеры для бизнеса, должны формировать положительный имидж в публичном пространстве для успешной реализации своих планов и проектов.

Взаимодействие Комитета с образовательными учреждениями должно стать системным и не ограничиваться частными мероприятиями просвещения в сфере цифровизации и информационной безопасности. Комитет при взаимодействии с имеющимися ресурсами ВУЗов может создать кадровую базу для развития процессов цифровизации в регионе.

В данном параграфе мы рассмотрели деятельность государственного органа в сфере информационной безопасности. Комитет цифрового развития представляет собой регулятор в сфере защиты информации, он определяет основные направления работы по защите информации в регионе. В его задачи входит методическое и техническое обслуживание информационной инфраструктуры государственных органов власти и обеспечение интересов жителей Ленинградской области.

В задачи Комитета входит обеспечение электронного документооборота всех органов власти Ленинградской области, обеспечение безопасности всех данных, используемых Правительством.

В процессе расширения сферы применения современных коммуникационных технологий Комитет цифрового развития Правительства ленинградской области становится одним из ключевых органов государственной власти.

Для реализации политики по обеспечению информационной безопасности Комитет сотрудничает с крупнейшими российскими компаниями по защите информации: Positive Technologies, ГК InfoWatch, Инфотекс, Лаборатория Касперского ( программное обеспечение по защите персональных компьютеров). Одной из задач Комитета является переход на отечественные программные продукты, поэтому приоритет отдается именно этим компаниям, лидерам в сфере информационной безопасности в России. Каждая компания имеет лицензии ФСБ и Министерства обороны РФ на разработку продуктов в сфере информационной безопасности. Комитет цифрового развития выстраивает систему сотрудничества как с местными региональными структурами, так и с всероссийскими, также он работает как с государственными органами, так и с частным сектором.

ЗАКЛЮЧЕНИЕ

На основе выдвигаемой нами во введении гипотезы мы проанализировали различные подходы к пониманию информационной безопасности, вызовы стоящие перед государственным управлением в эпоху цифровизации.

В первой главе мы определили, что основная цель цифровизации - обеспечение безопасности и повышение качества оказания государственных услуг. Одним из важнейших политических следствий цифровизации становится не только совершенствование системы предоставления государственных услуг, но и расширение участия граждан в принятии решений.

В России, в целом и в Ленинградской области, в частности, внедрение цифровых технологий замедленно в силу: запаздывания изменений необходимой нормативной базы, различной скорости внедрения цифровых технологий по отраслям, проблем в обеспечении информационной безопасности, недостатка квалифицированных кадров.

Информационная безопасность в России, с одной стороны это обеспечение безопасности государства и органов власти, с другой обеспечение защищенности каждого отдельного гражданина и компаний.

Во второй главе на основе рассмотренных программ мы можем сделать вывод о том, что необходимо организовывать непрерывное взаимодействие Правительства Ленинградской области в лице Комитета цифрового развития и ВУЗами региона для создания и совершенствования актуальных образовательных программ.

Для государственной службы необходимы кадры, не только имеющие hard skills в информационной безопасности, но и soft skills по обеспечению коммуникации между акторами и работе в команде. Государственная служба нуждается в кадрах, способных стать связующим звеном между государственной стратегией и конечным потребителем.

В третьей главе мы рассмотрели различные меры по обеспечению информационной безопасности в Ленинградской области. Проект «Территория БезОпасности» можно назвать одним из примеров, раскрывающий взгляд структурных подразделений Правительств Ленинградской области на проблемы информационной безопасности населения. Основным направлением деятельности проекта «Территория БезОпасности» в Ленинградской области является не только и не столько просвещение в сфере информационных пространств, продвижение и популяризация технического совершенствования мер по обеспечению информационной коллективной и личной безопасности в сети, сколько патриотическое воспитание молодежи. Основными угрозами при таком подходе являются управляемое протестное движение, декларативная поддержка "западных" ценностей и противопоставление их официальной политике руководства России.

Комитет цифрового развития Ленинградской области осуществляет, главным образом, техническое и административное регулирование в рамках обеспечения информационной безопасности в регионе. В задачи Комитета входит обеспечение электронного документооборота всех органов власти Ленинградской области, обеспечение безопасности всех данных, используемых Правительством. В процессе расширения сферы применения современных коммуникационных технологий Комитет цифрового развития Правительства ленинградской области становится одним из ключевых органов государственной власти.

На примере деятельности Комитета цифрового развития и проекта «Территория БезОпасности» мы видим двойственный подход к понимаю информационной безопасности. С одной стороны, профилирующий орган власти Ленинградской области развивающий техническую инфраструктуру по обеспечению безопасности и осуществляющий взаимодействие с частными компаниями в данной сфере, с другой стороны, социальная инициатива, поддержанная непрофильными комитетами, заключающая понимание информационной безопасности в попытку сохранения культурных ценностей граждан и отстаивание официального дискурса политики России.

Комитет цифрового развития, являясь одним из самых передовых в Правительстве Ленинградской области, на наш взгляд, недостаточное внимание уделяет продвижению и развитию имиджа Комитета в публичном пространстве. Комитет мало заметен в общественной сфере и поддержке социальных проектов и инициатив населения. Помимо информационной безопасности существует еще множество направлений деятельности Комитета, о которых можно было бы рассказать в публичном пространстве.

Формирование положительного имиджа организации, государственного органа, на наш взгляд, является одним из самых важных в условиях нового менеджмента и концепции governance. Государственные органы, выступающие как часть рынка услуг, как партнеры для бизнеса, должны формировать положительный имидж в публичном пространстве для успешной реализации своих планов и проектов.

Правительству Ленинградской области в лице Комитета цифрового развития организовать регулярное взаимодействие с ВУЗами для формирования и корректировки образовательных программ. Привлекать молодых специалистов в рамках организации мероприятий в виде круглых столов, кейс-чемпионатов, для отбора потенциальных сотрудников и формирования кадровой базы, а также популяризации деятельности Комитета и Правительства региона.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

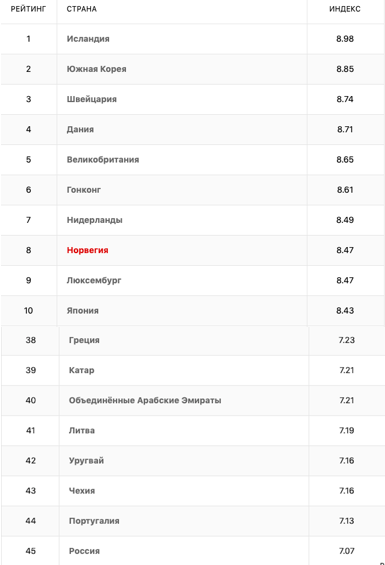
1. Asgarkhani, M. (2005). Digital Government and Its Effectiveness in Public Management Reform. Public Management Review, 7(3), С. 465–487.
2. Assange, J., Appelbaum, J., Muller-Maguhn, A. & Zimmermann, J. (2012). Cypherpunks: Freedom and the Future of the Internet. N.Y., L.: OR Books.
3. Brokeš, F. (2018, 24 September). Russia’s Sovereign Internet. Central European Financial Observer.
4. Castells M. The Rise of the Network Society. The Information Age. Economy, Society and Culture. Oxford: The Wiley-Blackwell. 2010. 656 p
5. Drake W. J., G. C. Vinton, Kleinwächter W. Future of the Internet Initiative. White Paper. Internet Fragmentation: An Overview // World Economic Forum, 2016.
6. Ganascia, J.-G. (2010). The Generalized Sousveillance Society. Social Science Information, 49(3), С. 489–507.
7. Hundley, Richard O., and Robert H. Anderson. "Emerging challenge: security and safety in cyberspace." In In Athena's Camp: Preparing for Conflict in the Information Age, edited by Arquilla John and Ronfeldt David, by Toffler Alvin and Toffler Heidi, RAND Corporation, 1997. P. 231-52.
8. Scott, B., Loonam, J. & Kumar, V. (2017). Exploring the Rise of Blockchain Technology: Towards Distributed Collaborative Organizations. Strategic Change, 26(5), 423–428.
9. Smorgunov, L., Neverov, K., & Kondratenko, K. (2019). Evolution of the Concept of Governability in the Context of Digitalization. В P. Kommers, & G. C. Peng (Ред.), Proceedings of the International Conference ICT, Society and Human Beings 2019, Smart Cities 2019 and Web Based Communities and Social Media 2019. (стр. 381-385). Porto: IADIS Press.
10. Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации»
11. Федеральный закон от 27.07.2004 г. No 79-ФЗ «О государственной гражданской службе Российской Федерации». Ст. 62.
12. Указ Президента РФ от 05.12.2016 No 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. No 50. Ст. 7074.
13. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»
14. Постановление Правительства Российской Федерации «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»» от 2.03.2019 г. №234
15. Областной закон Ленинградской области от 08.08.2016 N 76-оз (ред. от 19.12.2019) "О Стратегии социально-экономического развития Ленинградской области до 2030 года и признании утратившим силу областного закона "О Концепции социально-экономического развития Ленинградской области на период до 2025 года" (принят ЗС ЛО 13.07.2016)
16. Постановлением Правительства Ленинградской области от 05.08.2019 № 364 «Об утверждении положения о Комитете цифрового развития Ленинградской области и о признании утратившими силу отдельных постановлений Правительства Ленинградской области»
17. «Об утверждении квалификационных требований к профессиональным знаниям и навыкам, необходимым для исполнения должностных обязанностей по должностям государственной гражданской службы Ленинградской области в Представительстве Губернатора и Правительства Ленинградской области при Правительстве Российской Федерации»: Приказ от 12.05.2016 №4 //Представительство Губернатора и Правительства Ленинградской области при Правительстве Российской Федерации - 2016 - С.6
18. Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы раз- вития // Научно-технические ведомости СПбГПУ. Экономические науки. 2017. Т. 10, No 3. С. 9—25.
19. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования // М: Academia. 2004 г. 788 с.
20. Васильева Е.В., Пуляева В.Н., Юдина В.А. Развитие цифровых компетенций государственных гражданских служащих Российской Федерации // Бизнес-информатика. 2018. №4 (46)
21. Волкова А.В. Электронное правительство и формирование публичных ценностей в современной России // Вестник СПбГУ. Серия 6. Политология. Международные отношения. 2013. №3.
22. Гилева Т.А. Компетенции и навыки цифровой экономики: разработка программы развития персонала // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика . 2019. №2 (28)
23. Гуторов В. А., Радиков И. В. Концепции национальной безопасности в политическом дискурсе современной России: проблемы теории и методологии анализа // Вестник СПбГУ. Серия 6. Политология. Международные отношения. 2010. №4.
24. Гуторов В.А. Куда эволюционирует государство российское (методологические заметки) // Гуторов В.А. Политика: наука, философия, образование. – СПб., СПбГУ, Факультет политологии, 2011. – 516 с.
25. Игнатова А.М. Политические и концептуальные основания трансформации государственного управления в современной России: дис. … канд. полит. наук. СПбГУ, Санкт-Петербург, 2020.
26. Куприяновский В.П., Сухомлин В.А., Добрынин А.П., Райков А.Н., Шкуров Ф.В., Дрожжинов В.И., Федорова Н.О., Намиот Д.Е. Навыки в цифровой экономике и вызовы системы образования // International Journal of Open Information Technologies. 2017. №1.
27. Лаптев Л.Г. Бельков О.А. Образование и национальная безопасность // Вестник Московского университета. Серия 14. Психология. 2011. №4.
28. Сморгунов, Л. В. (2019). Партисипаторная управляемость и цифровизация. In С. Н. Васильев, & А. Д. Цвиркун (Eds.), Управление развитием крупномасштабных систем (MLSD’2019) [Электронный ресурс]: материалы Двенадцатой междунар. конфер, 1–3 окт. 2019 г., Москва / под общ. ред. С.Н. Васильева, А.Д. Цвиркуна ; Ин-т проблем упр. им. В.А. Трапезникова Рос. акад. наук . (pp. 1270-1273). Москва: Институт проблем управления им. В.А. Трапезникова РАН.
29. Сморгунов, Л. В. (2019). Институционализация управляемости и проблема контроля в пространстве цифровых коммуникаций. Южно-российский журнал социальных наук, 20(3), 62-75. [4].
30. Смотрицкая И.И. Государственное управление в условиях развития цифровой экономики: стратегические вызовы и риски // ЭТАП. 2018. №4.
31. Фомченкова Г.А. Информационно-идеологический фактор формирования духовной безопасности молодежи // Известия ВУЗов. Поволжский регион. Общественные науки. 2012. №1.
32. Юсупов Р.М. Шишкин В.М. Информационная безопасность, кибербезопасность и смежные понятия: cyber security vs информационной безопасности // Информационное противодействие угрозам терроризма. 2013 №21 С. 27-35

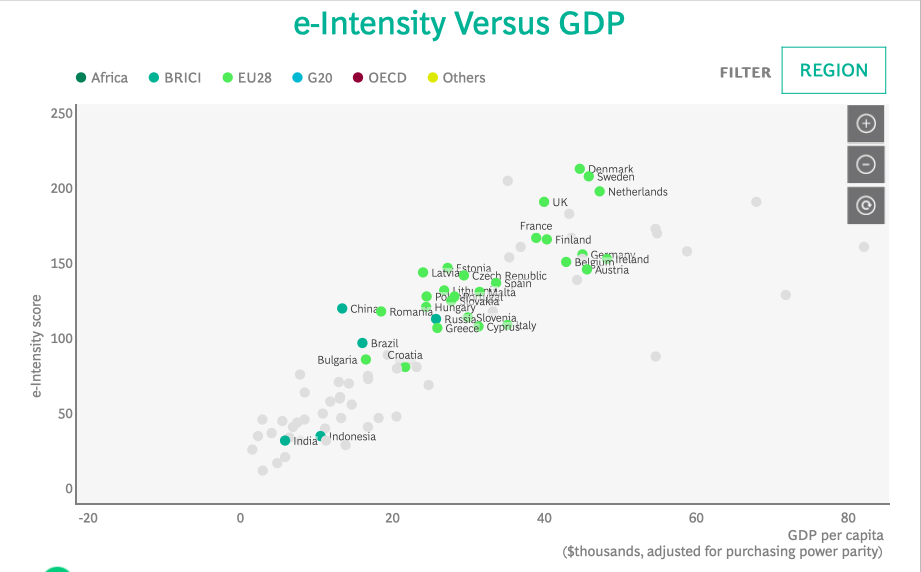
Список электронных источников

1. Positive Technologies. О продукте. URL: <https://www.ptsecurity.com/ru-ru/products/mpsiem/> (дата обращения 20.04.2020)
2. InfoWatch. О компании. URL: <https://www.infowatch.ru/company/about> (дата обращения 20.04.2020)
3. Более 13 тысяч госслужащих прошли обучение в Центре подготовки руководителей цифровой трансформации // Министерство цифрового развития, связи и массовых коммуникаций РФ URL: <https://digital.gov.ru/ru/events/39606/> (дата обращения 27.04.2020)
4. В Ленобласти оформлено более 1000 сделок с недвижимостью по технологии блокчейн. // URL: <https://rosreestr.ru/site/press/news/v-lenoblasti-oformleno-bolee-1000-sdelok-s-nedvizhimostyu-po-tekhnologii-blokcheyn/> (дата обращения 20.03.2020)
5. Георгиев Р. В мире тотальная нехватка специалистов по ИБ: спрос в полтора раза превышает предложение // C.News.Безопасность URL: <https://safe.cnews.ru/news/top/2019-11-13_v_mire_totalnaya_nehvatka> (дата обращения 27.04.2020)
6. ИнфоТеКС. О компании. URL: <https://infotecs.ru/about/> (дата обращения 20.04.2020)
7. Краснушкина Н. «Цифра» сопротивляется регулированию // Газета "Коммерсантъ" №118 от 09.07.2019 С.2. URL: <https://www.kommersant.ru/doc/4025324> (дата обращения 20.03.2020)
8. НАЦПРОЕКТЫ: регион внедряет «цифровые» решения 2019 г. URL: <https://lenobl.ru/ru/dlya-smi/news/22679/> ( дата обращения 22.05.2020)
9. Проект «Территория Безопасности» URL: [http://киберстандарт.рф/](http://xn--80aabndqn2azegmf.xn--p1ai/)  ( дата обращения 22.05.2020)
10. Проект «Территория БезОпасности. КиберАзбука» URL: [http://киберазбука.рф](http://xn--80aabbsndpg0dvb.xn--p1ai) (дата обращения 22.05.2020)
11. Прошин А. К чему ведет дефицит сотрудников в области информационной безопасности (и как с ним бороться) // ComNews Цифровая экономика URL: <http://www.comnews.ru/digital-economy/content/111783/2018-02-12/k-chemu-vedet-deficit-sotrudnikov-v-oblasti-informacionnoy-bezopasnosti-i-kak-s-nim-borotsya> ( дата обращения 27.04.2020)
12. Скандал с Facebook и Cambridge Analytica. Что мы знаем //BBC Русская служба 2018. URL: <https://www.bbc.com/russian/features-43475612> (дата обращения 20.05.2020)
13. «Текущее развитие проектов в сфере цифровой экономики в регионах России // Аналитический центр при Правительстве Российской Федерации 2019 г. URL: <https://ac.gov.ru/archive/files/publication/a/23243.pdf> (дата обращения 22.05.2020)
14. «Ъ» узнал о новой утечке данных клиентов Сбербанка // Интерфакс URL: <https://www.interfax.ru/business/681553> ( дата обращения 27.04.2020)
15. Юбилейный доклад декана экономического факультета МГУ имени М.В. Ломоносова, профессора А.А. Аузана «Цифровая экономика: фактор человеческого капитала» URL: https://www.econ.msu.ru/News.20190923192724\_8446/ ( дата обращения 22.05.2020)

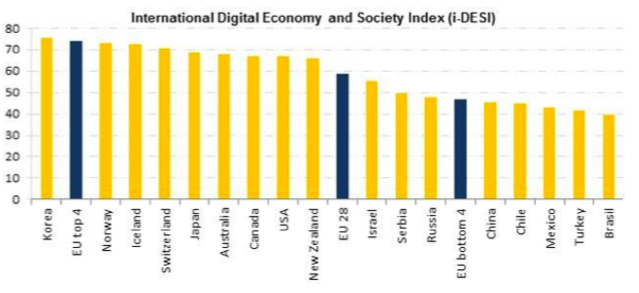
ПРИЛОЖЕНИЯ

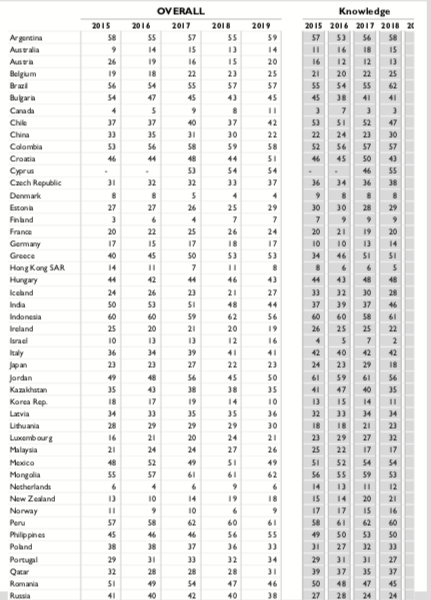
Приложение 1. ICT Development Index 2017.

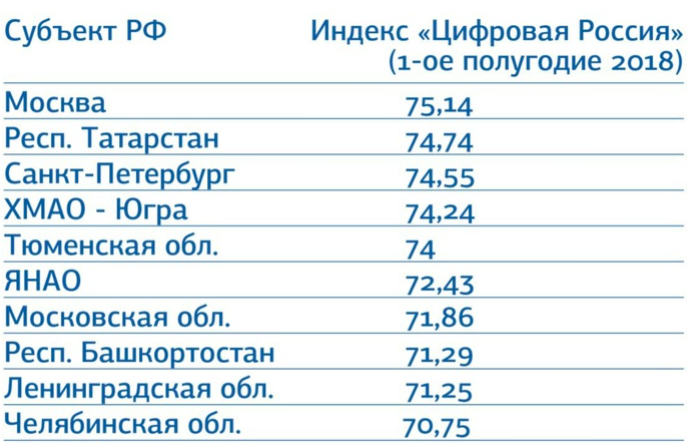


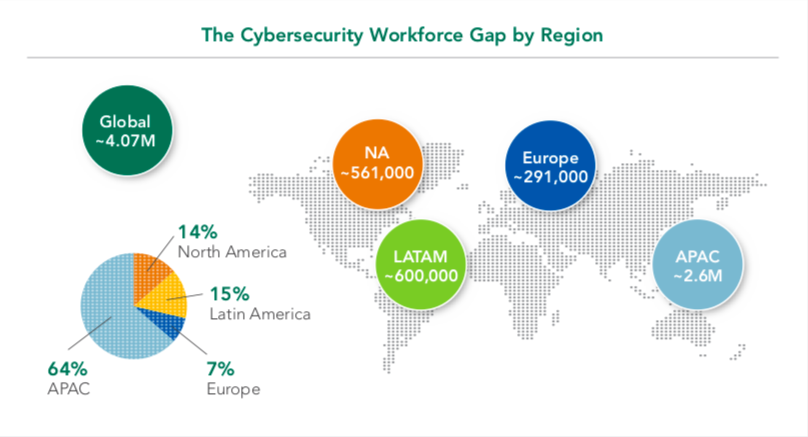
Приложение 2. BCG e-Intensity Index 2015.

Приложение 3. Международный индекс цифровой экономики и общества (I-DESI)



Приложение 4. IMD World Digital Competitiveness Ranking 2019.

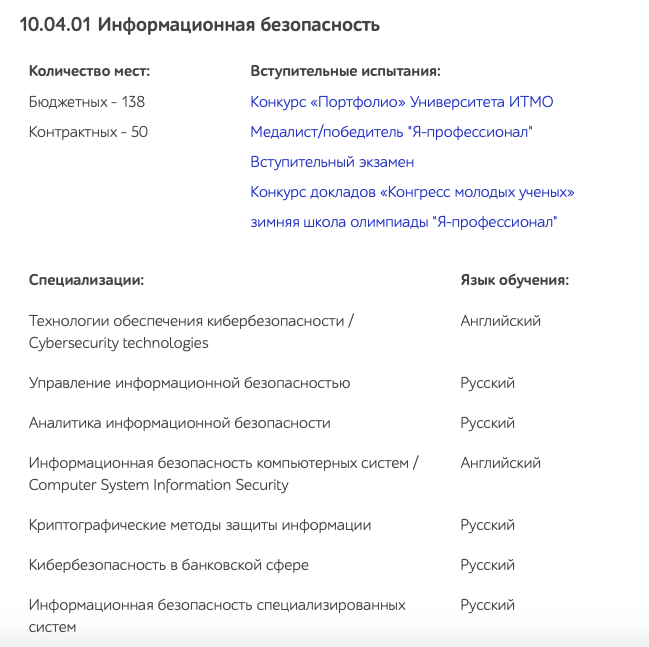
Приложение 5. Бизнес-школа «Сколково». Рейтинг регионов России по цифровизации 2018 г.

Приложение 6. Cybersecurity Workforce 2019. The Cybersecurity Workforce Gap by Region

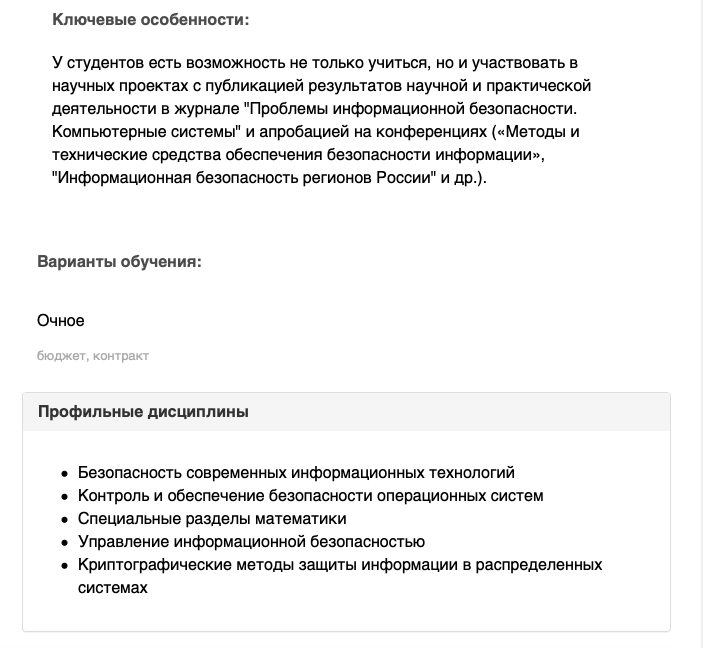
Приложение 7. Требуемые умения на должность государственной гражданской службы Ленинградской области главного специалиста отдела стратегических проектов департамента развития цифровых технологий Комитета  цифрового развития Ленинградской области 2020 г.

|  |  |
| --- | --- |
| Базовые | системного (стратегического) мышления; |
| систематизации и анализа информации |
| планирования, рационального использования служебного времени и достижения результатов |
| коммуникативного общения (в том числе публичных выступлений и ведения деловых переговоров; |
| управления изменениями |
| работы с аппаратным и программным обеспечением, установленном на  автоматизированном рабочем месте (АРМ), в том числе работы в операционной системе семейства Windows, в текстовом редакторе Microsoft Office Word, с табличным процессором Microsoft Office Excel, с почтовым клиентом типа «Outlook», подготовки презентаций с применением Microsoft Office PowerPoint; |
| работы в качестве пользователя в информационных системах, применяемых в комитете, в том числе в прикладных информационных системах (системе взаимодействия с гражданами и организациями, системе межведомственного электронного взаимодействия, учетной системе, информационно-аналитической системе, обеспечивающей сбор, обработку, хранение и анализ данных), системах электронного документооборота, в информационно-правовых системах «Гарант», «КонсультантПлюс», «Кодекс», а также с ресурсами и сервисами локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет» |
| использования копировальной техники, средств телефонной и факсимильной связи |
| в зависимости от области вида деятельности | подготовки аналитических, информационных и других материалов |
| подготовки методических рекомендаций, разъяснений |
| подготовки проектов правовых актов и обеспечение процедуры их согласования |
| подготовки заключений на проекты правовых актов |

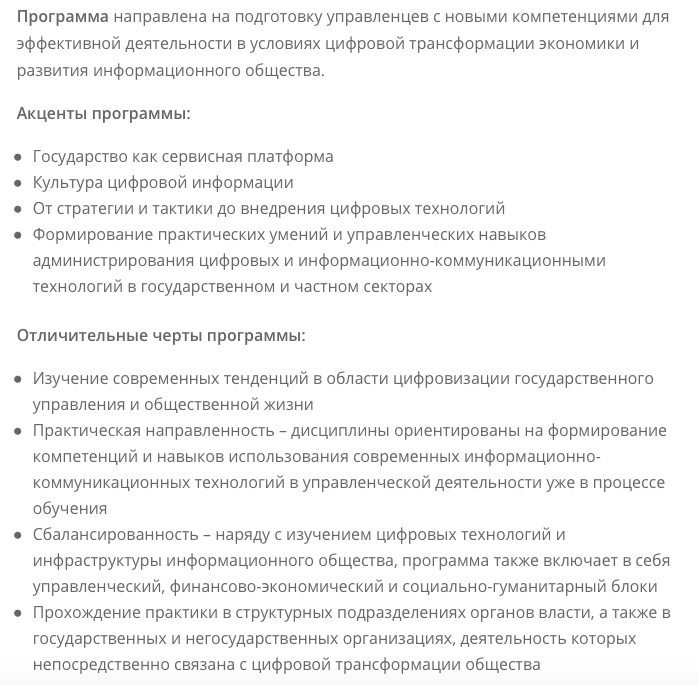
Приложение 8. Паспорт программы ИТМО 10.04.01 «Информационная безопасность»



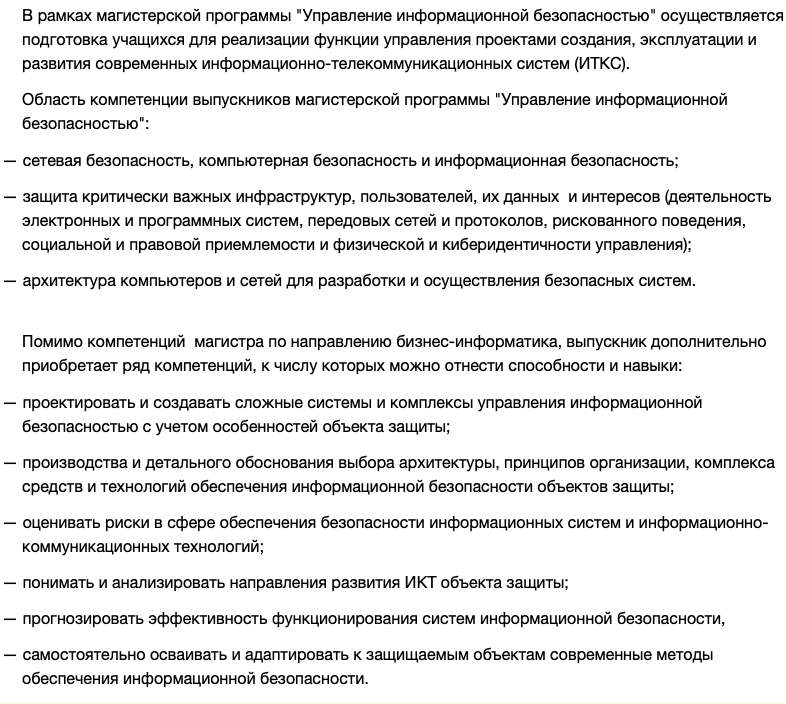
Приложение 9. Паспорт программы Санкт-Петербургский политехнический университет Петра Великого 10.04.01 « Информационная безопасность»



Приложение 10. Паспорт программы РАНХиГС 38.04.04. Государственное и муниципальное управление (ГМУ). Цифровое государство (стратегическое развитие информационного общества).



Приложение 11. Паспорт программы ВШЭ 38.04.05 Бизнес-информатика. Управление информационной безопасностью.



Приложение 12. Основные учебные курсы СПбГУ по программе 38.04.01 Управление бизнесом в цифровой экономике.

|  |
| --- |
| Менеджмент в цифровой экономике |
| Управленческий учет и аудит |
| Практики анализа данных |
| Цифровая экономика: современные вызовы |
| Цифровой маркетинг |
| Бизнес-анализ информации |
| Стратегия цифровой трансформации бизнеса |
| Стратегический маркетинг-менеджмент |
| Моделирование и управление бизнес-процессами |
| BI системы и управление данными |
| Индустрия 4.0 |
| Управление проектами |
| Управление организационными изменениями |
| Экономика цифрового предприятия |
| Цифровая культура: технологии и безопасность |
| Блокчейн |
| Имитационное моделирование экономических процессов |
| Информационная безопасность |
| Операционный менеджмент и управление цепочками поставок |
| Современные формы финансирования |
| Мотивационный менеджмент |
| Стратегия деловых переговоров |
| Оценка инвестиций в цифровой экономике |

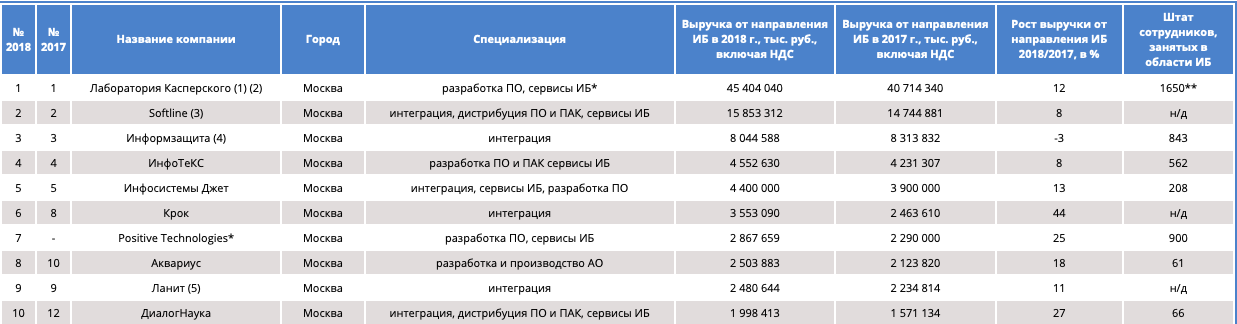
Приложение 13. Основные учебные курсы СПбГУ по программе 41.04.04 Цифровое публичное управление.

|  |
| --- |
| Основы программирования и алгоритмизации цифровых платформ |
| Социо-технические системы и публичная политика |
| Системы распределенных реестров и блокчейн-технологии в публичном управлении |
| Открытое правительство: сравнительный анализ |
| Дизайн публичной политики и управления в цифровом обществе |
| Краудсорсинговые технологии и принятие политико-управленческих решений |
| Геоинформационные системы и управление территориями |
| Технологии искусственного интеллекта для поддержки принятия решений |
| Умное управление городами |
| Цифровое инновационное управление |
| Публичные услуги и цифровая экономика совместного пользования |
| Гражданская наука и участие в цифровой публичной политике |
| Инициативное гражданское бюджетирование: онлайн платформы |

Приложение 14. Структура Комитета цифрового развития Ленинградской области.



Приложение 15. CNews Security: Крупнейшие компании России в сфере защиты информации 2019



1. Игнатова А.М. Политические и концептуальные основания трансформации государственного управления в современной России: дис. … канд. полит. наук. СПбГУ, Санкт-Петербург, 2020. [↑](#footnote-ref-1)
2. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования // М: Academia. 2004 г. 788 с. [↑](#footnote-ref-2)
3. Castells M. The Rise of the Network Society. The Information Age. Economy, Society and Culture. Oxford: The Wiley-Blackwell. 2010. 656 p [↑](#footnote-ref-3)
4. Сморгунов, Л. В. (2019). Партисипаторная управляемость и цифровизация. In С. Н. Васильев, & А. Д. Цвиркун (Eds.), Управление развитием крупномасштабных систем (MLSD’2019) [Электронный ресурс]: материалы Двенадцатой междунар. конфер, 1–3 окт. 2019 г., Москва / под общ. ред. С.Н. Васильева, А.Д. Цвиркуна ; Ин-т проблем упр. им. В.А. Трапезникова Рос. акад. наук . (pp. 1270-1273). Москва: Институт проблем управления им. В.А. Трапезникова РАН. [↑](#footnote-ref-4)
5. Сморгунов, Л. В. (2019). Институционализация управляемости и проблема контроля в пространстве цифровых коммуникаций. Южно-российский журнал социальных наук, *20*(3), 62-75. [4]. [↑](#footnote-ref-5)
6. Скандал с Facebook и Cambridge Analytica. Что мы знаем //BBC Русская служба 2018. [↑](#footnote-ref-6)
7. Смотрицкая И.И. Государственное управление в условиях развития цифровой экономики: стратегические вызовы и риски // ЭТАП. 2018. №4. [↑](#footnote-ref-7)
8. Волкова А.В. Электронное правительство и формирование публичных ценностей в современной России // Вестник СПбГУ. Серия 6. Политология. Международные отношения. 2013. №3. [↑](#footnote-ref-8)
9. Сморгунов, Л. В. (2019). Институционализация управляемости и проблема контроля в пространстве цифровых коммуникаций. Южно-российский журнал социальных наук, *20*(3), 62-75. [4]. [↑](#footnote-ref-9)
10. Asgarkhani, M. (2005). Digital Government and Its Effectiveness in Public Management Reform. *Public Management Review*, 7(3), С. 465–487. [↑](#footnote-ref-10)
11. Ganascia, J.-G. (2010). The Generalized Sousveillance Society. *Social Science Information*, 49(3), С. 489–507. [↑](#footnote-ref-11)
12. Smorgunov, L., Neverov, K., & Kondratenko, K. (2019). Evolution of the Concept of Governability in the Context of Digitalization. В P. Kommers, & G. C. Peng (Ред.), *Proceedings of the International Conference ICT, Society and Human Beings 2019, Smart Cities 2019 and Web Based Communities and Social Media 2019.* (стр. 381-385). Porto: IADIS Press. [↑](#footnote-ref-12)
13. Scott, B., Loonam, J. & Kumar, V. (2017). Exploring the Rise of Blockchain Technology: Towards

    Distributed Collaborative Organizations. *Strategic Change*, 26(5), 423–428. [↑](#footnote-ref-13)
14. Assange, J., Appelbaum, J., Muller-Maguhn, A. & Zimmermann, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. N.Y., L.: OR Books. [↑](#footnote-ref-14)
15. Drake W. J., G. C. Vinton, Kleinwächter W. Future of the Internet Initiative. White Paper. Internet Fragmentation: An Overview // World Economic Forum, 2016.  [↑](#footnote-ref-15)
16. Гуторов В.А. Куда эволюционирует государство российское (методологические заметки) // Гуторов В.А. Политика: наука, философия, образование. – СПб., СПбГУ, Факультет политологии, 2011. – 516 с.

    [↑](#footnote-ref-16)
17. Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы раз- вития // Научно-технические ведомости СПбГПУ. Экономические науки. 2017. Т. 10, No 3. С. 9—25. [↑](#footnote-ref-17)
18. Постановление Правительства Российской Федерации «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»» от 2.03.2019 г. №234 [↑](#footnote-ref-18)
19. Краснушкина Н. «Цифра» сопротивляется регулированию // Газета "Коммерсантъ" №118 от 09.07.2019 С.2. URL: <https://www.kommersant.ru/doc/4025324> (дата обращения 20.03.2020) [↑](#footnote-ref-19)
20. В Ленобласти оформлено более 1000 сделок с недвижимостью по технологии блокчейн. // URL: <https://rosreestr.ru/site/press/news/v-lenoblasti-oformleno-bolee-1000-sdelok-s-nedvizhimostyu-po-tekhnologii-blokcheyn/> (дата обращения 20.03.2020) [↑](#footnote-ref-20)
21. «Текущее развитие проектов в сфере цифровой экономики в регионах России // Аналитический центр при Правительстве Российской Федерации 2019 г. URL: <https://ac.gov.ru/archive/files/publication/a/23243.pdf> (дата обращения 22.05.2020) [↑](#footnote-ref-21)
22. НАЦПРОЕКТЫ: регион внедряет «цифровые» решения 2019 г. URL: <https://lenobl.ru/ru/dlya-smi/news/22679/> ( дата обращения 22.05.2020) [↑](#footnote-ref-22)
23. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [↑](#footnote-ref-23)
24. Указ Президента РФ от 05.12.2016 No 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. No 50. Ст. 7074. [↑](#footnote-ref-24)
25. Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [↑](#footnote-ref-25)
26. Brokeš, F. (2018, 24 September). Russia’s Sovereign Internet. *Central European Financial Observer*. [↑](#footnote-ref-26)
27. Юбилейный доклад декана экономического факультета МГУ имени М.В. Ломоносова, профессора А.А. Аузана «Цифровая экономика: фактор человеческого капитала» URL: <https://www.econ.msu.ru/News.20190923192724_8446/> ( дата обращения 22.05.2020) [↑](#footnote-ref-27)
28. Георгиев Р. В мире тотальная нехватка специалистов по ИБ: спрос в полтора раза превышает предложение // C.News.Безопасность URL: <https://safe.cnews.ru/news/top/2019-11-13_v_mire_totalnaya_nehvatka> (дата обращения 27.04.2020) [↑](#footnote-ref-28)
29. Прошин А. К чему ведет дефицит сотрудников в области информационной безопасности (и как с ним бороться) // ComNews Цифровая экономика URL: <http://www.comnews.ru/digital-economy/content/111783/2018-02-12/k-chemu-vedet-deficit-sotrudnikov-v-oblasti-informacionnoy-bezopasnosti-i-kak-s-nim-borotsya> ( дата обращения 27.04.2020) [↑](#footnote-ref-29)
30. "Ъ" узнал о новой утечке данных клиентов Сбербанка // Интерфакс URL: <https://www.interfax.ru/business/681553> ( дата обращения 27.04.2020) [↑](#footnote-ref-30)
31. Гилева Т.А. Компетенции и навыки цифровой экономики: разработка программы развития персонала // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика . 2019. №2 (28) [↑](#footnote-ref-31)
32. Васильева Е.В., Пуляева В.Н., Юдина В.А. Развитие цифровых компетенций государственных гражданских служащих Российской Федерации // Бизнес-информатика. 2018. №4 (46) [↑](#footnote-ref-32)
33. Федеральный закон от 27.07.2004 г. No 79-ФЗ «О государственной гражданской службе Российской Федерации». Ст. 62. [↑](#footnote-ref-33)
34. Более 13 тысяч госслужащих прошли обучение в Центре подготовки руководителей цифровой трансформации // Министерство цифрового развития, связи и массовых коммуникаций РФ URL: <https://digital.gov.ru/ru/events/39606/> (дата обращения 27.04.2020) [↑](#footnote-ref-34)
35. Васильева Е.В., Пуляева В.Н., Юдина В.А. Развитие цифровых компетенций государственных гражданских служащих Российской Федерации // Бизнес-информатика. 2018. №4 (46) [↑](#footnote-ref-35)
36. Об утверждении квалификационных требований к профессиональным знаниям и навыкам, необходимым для исполнения должностных обязанностей по должностям государственной гражданской службы Ленинградской области в Представительстве Губернатора и Правительства Ленинградской области при Правительстве Российской Федерации: Приказ от 12.05.2016 №4 //Представительство Губернатора и Правительства Ленинградской области при Правительстве Российской Федерации - 2016 - С.6 [↑](#footnote-ref-36)
37. Юбилейный доклад декана экономического факультета МГУ имени М.В. Ломоносова, профессора А.А. Аузана «Цифровая экономика: фактор человеческого капитала» URL: <https://www.econ.msu.ru/News.20190923192724_8446/> ( дата обращения 22.05.2020) [↑](#footnote-ref-37)
38. Областной закон Ленинградской области от 08.08.2016 N 76-оз (ред. от 19.12.2019) "О Стратегии социально-экономического развития Ленинградской области до 2030 года и признании утратившим силу областного закона "О Концепции социально-экономического развития Ленинградской области на период до 2025 года" (принят ЗС ЛО 13.07.2016) [↑](#footnote-ref-38)
39. Hundley, Richard O., and Robert H. Anderson. "Emerging challenge: security and safety in cyberspace." In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by Arquilla John and Ronfeldt David, by Toffler Alvin and Toffler Heidi, RAND Corporation, 1997. P. 231-52. [↑](#footnote-ref-39)
40. Гуторов В. А., Радиков И. В. Концепции национальной безопасности в политическом дискурсе современной России: проблемы теории и методологии анализа // Вестник СПбГУ. Серия 6. Политология. Международные отношения. 2010. №4. [↑](#footnote-ref-40)
41. Юсупов Р.М. Шишкин В.М. Информационная безопасность, кибербезопасность и смежные понятия: cyber security vs информационной безопасности // Информационное противодействие угрозам терроризма. 2013 №21 С. 27-35 [↑](#footnote-ref-41)
42. Лаптев Л.Г. Бельков О.А. Образование и национальная безопасность // Вестник Московского университета. Серия 14. Психология. 2011. №4. [↑](#footnote-ref-42)
43. Проект «Территория Безопасности» URL: [http://киберстандарт.рф/](http://xn--80aabndqn2azegmf.xn--p1ai/)  ( дата обращения 22.05.2020) [↑](#footnote-ref-43)
44. Куприяновский В.П., Сухомлин В.А., Добрынин А.П., Райков А.Н., Шкуров Ф.В., Дрожжинов В.И., Федорова Н.О., Намиот Д.Е. Навыки в цифровой экономике и вызовы системы образования // International Journal of Open Information Technologies. 2017. №1. [↑](#footnote-ref-44)
45. «Территория БезОпасности. КиберАзбука» URL: [http://киберазбука.рф](http://xn--80aabbsndpg0dvb.xn--p1ai) (дата обращения 22.05.2020) [↑](#footnote-ref-45)
46. Фомченкова Г.А. Информационно-идеологический фактор формирования духовной безопасности молодежи // Известия ВУЗов. Поволжский регион. Общественные науки. 2012. №1. [↑](#footnote-ref-46)
47. Постановлением Правительства Ленинградской области от 05.08.2019 № 364 «Об утверждении положения о Комитете цифрового развития Ленинградской области и о признании утратившими силу отдельных постановлений Правительства Ленинградской области» [↑](#footnote-ref-47)
48. Positive Technologies. О продукте. URL: <https://www.ptsecurity.com/ru-ru/products/mpsiem/> (дата обращения 20.04.2020) [↑](#footnote-ref-48)
49. ИнфоТеКС. О компании. URL: <https://infotecs.ru/about/> (дата обращения 20.04.2020) [↑](#footnote-ref-49)
50. InfoWatch. О компании. URL: <https://www.infowatch.ru/company/about> (дата обращения 20.04.2020) [↑](#footnote-ref-50)