ЦИФРОВАЯ ЭКОНОМИКА

Учебник

Под редакцией доктора экономических наук,
профессора **Л. А. Каргиной**

Для студентов, обучающихся по направлениям подготовки
38.03.01. «Экономика» и 38.03.02 «Менеджмент»
(Квалификация (степень) «бакалавр»)

Рекомендовано УМО
в качестве учебника для вузов

ИЗДАТЕЛЬСТВО Прометей

МОСКВА
2020

УДК 330
ББК 65
Ц 75

Авторы-составители:

Каргина Л. А., д.э.н., профессор, ***Вовк А. А.***, д.э.н., профессор, ***Лебедева С. Л.***, к.ф.-м.н., доцент (Введение); ***Дмитриева Т. М.*** (Глава 1); гл. 2 — ***Демидов А. В.***, к.э.н. (Глава 2); ***Медникова О. В.***, к.т.н., ***Алексеенко М. Я.*** (Глава 3, пп. 3.1—3.3); ***Соколова И. И.***, к.э.н., доцент, ***Бритвин М. А.*** (Глава 3, п. 3.4); — гл. 4 — ***Морозова В. И.***, к.э.н., доцент, ***Вишневский К. Э.*** (Глава 4); ***Каргина Л. А.***, д.э.н., ***Лебедева*** . профессор, к.ф.-м.н., доцент (Глава 5); ***Михненко О. Е.***, д. э.н., профессор (Глава 6);

Рецензенты:

Ц 75 **Цифровая экономика:** Учебник / Авторы-составители: Л. А. Каргина, С. Л. Лебедева [и др.]; под ред. Л. А. Каргиной. — М.: Прометей, 2020. — 220 с.

В учебнике раскрыта сущность цифровой экономики, рассматривается совокупность взаимосвязанных понятий, принципов, методов и методик, нормативно-правового регулирования, охватывающих различные аспекты практики управления в современных условиях, как на уровне предоставления государственных услуг и сервисов, так и на уровне управления электронным бизнесом. Излагаются основные положения по характеристике цифрового государства, построения цифрового профиля гражданина и организации, необходимых для развития единой цифровой государственной облачной платформы и платформ предоставления государственных и коммерческих услуг организаций, а также вопросы информационной безопасности с учетом результатов рыночных преобразований на транспорте, а также с целью разработки методики использования цифровых технологий. Включен практический материал.

Настоящий учебник соответствует требованиям, изложенным в Федеральном образовательном стандарте высшего профессионального образования последнего поколения.

Для студентов высших учебных заведений обучающихся по направлениям «Экономика» и «Менеджмент».

ISBN

ОГЛАВЛЕНИЕ

Введение **5**

Глава 1. Цифровое государство **8**
1.1. Цифровое и электронное государство, электронное правительство 8
1.2. Государственная единая облачная платформа 16
1.3. Модели и платформы предоставления государственных услуг 29
1.4. Мобильная и облачная электронные цифровые подписи 32
Вопросы для самоконтроля 36
Список использованных источников главы 1 36

Глава 2. Построение цифрового профиля гражданина и организации для развития цифровых государственных и коммерческих услуг **39**
2.1. Понятие, цели и принципы создания цифрового профиля 39
2.2. IT-архитектура и механизм работы цифрового профиля 49
2.3. Обеспечение информационной безопасности цифрового профиля 64
Вопросы для самоконтроля 80
Список использованных источников главы 2 81

Глава 3. Цифровые технологии **83**
3.1. История развития цифровых технологий 83
3.2. Сферы применения цифровых технологий 86
3.3. Наука о данных 99
3.4. Решение задач машинного обучения 115
Вопросы для самоконтроля 130
Список использованных источников главы 3 131

Глава 4. Информационная безопасность в цифровой экономике **135**
4.1. Предмет и объект защиты 136
4.2. Методы и средства защиты информации 140

4.3. Управление доступом. Идентификация и аутентификация 144
4.4. Криптография и стеганография 147
4.5. Компьютерные вирусы антивирусная защита. Ответственность за компьютерные преступления 161
Вопросы для самоконтроля 168
Список использованных источников главы 4 170
5.1. Стартапы. Характеристики, компоненты, отличительные особенности 172
5.2. Кейсы цифровой трансформации 177
Вопросы для самоконтроля 187
Список использованных источников главы 5 187
Глава 6. Кадры для цифровой экономики 189
6.1. Задачи развития цифровой экономики 189
6.2. Компетенции цифровой экономики 193
6.3. Система уровней квалификаций для цифровых компетенций 196
Вопросы для самоконтроля 210
Список использованных источников главы 6 211
Практикум. Методические указания по написанию рефератов 212

ВВЕДЕНИЕ

Вопросы цифровой экономики на транспорте имеют особую значимость в силу особенностей организации производственных процессов и специфики условий производства. В настоящем учебнике с целью определения направлений развития цифровой экономики и применения ее принципов излагаются актуальные положения по характеристике цифрового государства, построения цифрового профиля гражданина и организации, необходимых для развития единой цифровой государственной облачной платформы и платформ предоставления государственных и коммерческих услуг организаций, вопросы информационной безопасности с учетом результатов рыночных преобразований на транспорте, а также с целью, использования методов анализа данных.

Цифровая экономика как учебная дисциплина занимает важное место в процессе подготовки бакалавров по направлению «Экономика» и «Менеджмент». Это обусловлено тем, что для управления производственными процессами необходимо понимание места и роли цифровых бизнес-моделей и экосистем в процессе производства и управления. Под цифровой экономикой понимается экономическая деятельность, функционирование которой основывается на цифровых технологиях с использованием соответствующих бизнес-процессов и моделей, при этом основная деятельность заключается не только в разработке и продаже программных продуктов, но и в производимых электронных товарах и сервисах. По определению Всемирного банка, цифровая экономика — это система экономических, социальных и культурных отношений, основанных на использовании цифровых информационно-коммуникативных технологий. Важнейшее место в цифровой экономике занимает цифровое государство, как важнейший элемент цифровой экономики, поскольку только благодаря использованию цифровых технологий обеспечивается информационная безопасность. Именно

этим обусловливается значительное внимание, которое уделялось вопросам организации цифрового и электронного государства, созданию государственной единой облачной платформы, моделей и платформ предоставления государственных и коммерческих услуг и цифровой подписи на всех этапах их формирования.

Вопросы развития цифровой экономики являются объектом пристального внимания ученых и практиков в течение ряда лет. Об этом свидетельствует наличие значительного количества публикаций самых различных по значимости и глубине изучения проблем (от популярных статей до диссертационных исследований) по вопросам цифровой экономики.

Главным условием обеспечения эффективности цифровой экономики становится внедрение прогрессивных технологий обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг.

В связи с этим учебник может быть использован при изучении курса цифровой экономики, а также при самостоятельном изучении методологии цифровой экономики, и соответствия принципов организации и ведения цифровой экономики, изложенных в учебнике, принципам, применяемым на практике. При этом надо исходить из того, что положения теории единообразны и применимы не только в транспортных компаниях, но и в компаниях других отраслей экономики.

Наряду с этим в соответствии со сформулированными в учебнике положениями раскрывается сущность цифровой экономики и вопросы применения на транспорте ее принципов.

Учебник подготовлен в соответствии с программой курса «Цифровая экономика», предусмотренного учебными планами и образовательными стандартами подготовки бакалавров, по направлениям «Экономика» и «Менеджмент» и может быть полезен аспирантам, научным работникам и специалистам-практикам.

Основной задачей учебного издания является формирование у студентов способности осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач и использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ

В результате освоения дисциплины «Цифровая экономика» студент будет:

знать и понимать:

– основные принципы и методы сбора, отбора и обобщения информации;

– методы обработки и интеллектуального анализа крупных массивов данных;

уметь:

– находить и критически анализировать информацию, необходимую для решения задач профессиональной деятельности;

– соотносить разнородные явления и систематизирует их в рамках избранных видов профессиональной деятельности;

– применять навыки использования современных информационных и коммуникационных технологий и программных средств при решении профессиональных задач;

владеть навыками:

– использования современных информационных и коммуникационных технологий и программных средств при решении профессиональных задач;

– рассматривать и предлагать возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки.

Глава 1
ЦИФРОВОЕ ГОСУДАРСТВО

В государственном секторе повсеместно используются информационно-коммуникационные технологии. Поскольку цифровые технологии облегчают распространение информации и предоставляют возможность обратной связи, они являются идеальным каналом для налаживания партнерских отношений между гражданами и правительствами в целях повышения общественной ценности.

Сегодня на всех уровнях государственного управления активно применяются информационные технологии и системы для решения задач граждан, сотрудников государственных организаций, бизнеса.

1.1. Цифровое и электронное государство, электронное правительство

Цифровое государство включает в себя электронное правительство, реализация которого связана с разработкой новых методов и подходов для эффективного взаимодействия граждан и бизнеса с госструктурами.

Цифровое государство — это и предоставление государственных услуг сотрудникам (G2E) — государственным служащим по обеспечению их обучения и др. аспектов развития человеческих ресурсов, в том числе гражданам (G2C) с использованием электронного документооборота и возможностей веб-сайтов, участие граждан в процессе консультаций и принятия решений и межведомственное

взаимодействие, которое предполагает обмен данными между многочисленными информационными системами различных ведомств и организаций (G2G), и взаимодействие государства и бизнеса (G2B), например, платежи, продажа и покупка товаров и услуг, а также предоставление услуг, ориентированных на бизнес.

Основные области для реализации инициатив электронного правительства представлены ниже.

1. Совершенствование процессов государственного управления: электронное администрирование — инициативы электронного правительства в этой области касаются, в частности, улучшений внутренней работы государственного сектора:

– Сокращения затрат на процессы: улучшение соотношения «затраты-выпуск» путем сокращения финансовых затрат и/или временных затрат.

– Управления производительностью процессов: планирование, мониторинг и контроль эффективности использования технологических ресурсов (людских, финансовых и других).

– Налаживания стратегических связей в правительстве: установление связей между учреждениями, уровнями правительства в целях укрепления потенциала по разработке и осуществлению стратегии и политики, определяющих процессы управления.

2. Подключение граждан: eCitizens и eServices.

Такие инициативы касаются, в частности, взаимоотношений между правительством и гражданами: либо в качестве избирателей/заинтересованных сторон, от которых государственный сектор должен получать свою легитимность, либо в качестве клиентов, потребляющих государственные услуги. Эти инициативы вполне могут включать усовершенствования процесса. Они также включают в себя более широкие полномочия:

– Диалог с гражданами: предоставление гражданам подробной информации о деятельности государственного сектора. Это касается главным образом определенных

видов подотчетности: повышения ответственности государственных служащих за принимаемые ими решения и принимаемые ими меры.

– Сбор мнений граждан: увеличение вклада граждан в решения и действия государственного сектора, демократизация процессов принятия решений.

– Улучшение государственных услуг: улучшение услуг, предоставляемых представителям общественности по таким параметрам, как качество, удобство и стоимость.

3. Построение внешних взаимодействий: eSociety.

Рис. 1.1. Три основных аспекта в инициативах электронного правительства [1]

Такие инициативы касаются, в частности, взаимоотношений между государственными учреждениями и другими институтами — другими государственными учреждениями, компаниями частного сектора, некоммерческими и общественными организациями:

– Более эффективная работа с бизнесом: улучшение взаимодействия между государством и бизнесом. Это включает в себя оцифровку регулирования, закупок и услуг для бизнеса с целью повышения качества и удобства.

– Налаживание партнерских отношений: создание организационных групп для достижения экономических и социальных целей.

Цифровое правительство подразумевает новые стили руководства, трансформацию способов предоставления услуг, взаимодействия граждан и государства.

Функции бэк-офиса электронного правительства могут быть организованы по-разному для обслуживания различных пользовательских услуг от простых сервисов взаимодействия до взаимодействий между различными правительственными организациями, что подразумевает как вертикальную, так и горизонтальную интеграцию, включая как централизованные, так и децентрализованные решения.

Историческая ретроспектива

Впервые термин «электронное правительство» был использован в выступлении президента США Билла Клинтона в 1992 году.

Инициатива администрации США «Совершенствование правительственной деятельности через новые технологии» была заявлена в феврале 1997 г. Разработка методики федеральной архитектуры США — FEAF — началась в 1998 г. В ней реализован функциональный подход (со стороны бизнес-процессов).

FEAF создавалась как основа для разработки стандартов совместимости, процессов и обмена информацией госорганов и организаций.

В Германии задача реализации электронного правительства решается с 2000 г., когда были разработаны стандарты и архитектура прикладных систем электронного правительства — SAGA.

В Великобритании в 2000 году был выпущен стандарт e-GIF — Среда Межведомственного Взаимодействия Правительства. В 2011 г. была основана Цифровая служба Правительства Великобритании — GDS.

В 2012 г. был запущен портал GOV.UK, заменивший сервис электронного правительства.

Активно ведутся работы по реализации «правительства как платформы»: предоставлению стандартизированных

цифровых услуг, таких как проверка личности, коммуникация пользователей и онлайн-платежи, для использования во всех правительственных ведомствах.

Правительственное облако в Великобритании (G-Cloud) служит для поиска поставщиков технологий и приобретения услуг, связанных с правительством. Государственные учреждения могут приобретать услуги у поставщиков облачных вычислений, таких как, AWS, Microsoft, Google. В рамках G-Cloudframework организации могут выбирать облачный хостинг (IaaS, PaaS), облачное программное обеспечение (SaaS), облачную поддержку и техническое обслуживание облачного хостинга и программного обеспечения. Покупатели могут заключить контракт с выбранным поставщиком услуг.

В Австралии функционирует FedLink — правительственный шлюз и защищенный правительственный Интернет.

Один из признанных лидеров на пути к построению цифрового государства — Сингапур. В 80-х годах XX в. в рамках реализации национального плана по «компьютеризации» был создан Национальный компьютерный совет (NCB), который в числе других направлений своей деятельности занимается компьютеризацией госуслуг. Затем была сформирована стратегия IT2000 Masterplan и предложен «План действий по внедрению концепции цифрового государства» на 2000—2003 годы.

Например, уже с 2003 года все жители Сингапура в возрасте от 15 лет могут подать заявку на получение SingPass — цифрового удостоверения личности для совершения операций с правительственным порталом онлайн-услуг.

В Японии в 1997 году была введена единая информационная платформа, которая объединила министерства и ведомства — WAN Kasumigaseki. Важным шагом для распространения концепции цифрового государства стало принятие в 2000 году Хартии глобального информационного общества. Главная мысль заключалась в том, что всем людям должны быть доступны блага этого общества. Документ был предложен к подписанию членам Большой восьмерки. Россия стала одной из стран, подписавших Хартию.

В период с 1999 по 2005 год правительство предложило несколько направлений развития цифрового государства: Основные принципы общества, основанного на информации и коммуникациях; программа e-Japan, объединяющая все меры по построению цифрового общества; и программа по построению цифрового государства.

Аналогичные проекты развиваются и в других странах.

Уровень развития e-government, ИКТ, готовность к сетевому обществу можно оценить по авторитетным международным рейтингам, в числе которых рейтинги Организации объединенных наций (ООН), представленные на сайте http://unpan.org/, Международного союза электросвязи (МСЭ) на сайте itu.int, Всемирного экономического форума (ВЭФ) — reports.weforum.org.

Состав электронного правительства

Федеральная целевая программа «Электронная Россия на 2002—2010 годы» была разработана в России в 2001 году. В ней рассматриваются все сферы информатизации в стране, в том числе введение электронного правительства. Состав электронного правительства определяется в законопроекте о единой инфраструктуре электронного правительства.

Состав электронного правительства включает в себя следующие компоненты (рис. 1.1).

Цифровое правительство

В апреле 2016 года сотрудниками Всемирного банка совместно с Институтом развития информационного общества был подготовлен доклад «Цифровое правительство 2020. Перспективы для России», в котором приводится определение цифрового правительства компании «Гартнер»:

Государственные информационные системы электронного правительства	Единый портал государственных и муниципальных услуг (функций) Головной удостоверяющий центр Единая система идентификации и аутентификации (ЕСИА) Единая система межведомственного электронного взаимодействия (СМЭВ) Система досудебного обжалования Единая система нормативной справочной информации (ЕСНСИ) Государственная электронная почта
Техническая инфраструктура	Центры обработки данных Система информационной безопасности Сеть передачи данных органов государственной власти
Государственная инфраструктура облачных вычислений	Информационная система «Платформа хранения электронных документов» Информационная система мониторинга функционирования инфраструктуры электронного правительства

Рис. 1.1. Состав электронного правительства

«Цифровое правительство — правительство, создаваемое и действующее так, чтобы использовать преимущества цифровых данных при оптимизации, трансформации и создании государственных услуг».

Характеристики цифрового правительства представлены далее (рис. 1.2).

Принцип предоставления услуг электронного правительства, являющихся цифровыми по умолчанию, подразумевает применение перепроектирования и реинжиниринга административных процессов для повышения эффективности оказываемых гражданам и предприятиям услуг.

Принципы предоставления услуг цифрового правительства	Цифровые по умолчанию Платформонезависимость и ориентация на мобильные устройства Проектирование услуг, ориентированное на пользователя Цифровые от начала до конца Правительство как платформа
Основные элементы цифрового правительства	Единый портал Единые данные для совместного использования в государственном секторе Межведомственные сервисы для совместного использования Государственная инфраструктура совместного использования Улучшенные сенсорные сети и аналитика Кибербезопасность и конфиденциальность

Рис. 1.2. Характеристики цифрового правительства [2]

При проектировании нужно ориентироваться на использование клиентами мобильных устройств.

Дальнейшее развитие «интернета вещей» позволит накапливать и анализировать большое количество информации о жизненных обстоятельствах людей и среде их проживания. Это приведет к тому, что услуги станут еще более индивидуализированы с детальным пониманием нужд пользователей услуг. Поэтому проектирование услуг должно быть ориентировано на пользователя.

Процессы как фронт-офиса, так и бэк-офиса цифрового правительства должны обеспечивать наличие полностью цифрового административного процесса для реализации принципа предоставления цифровых услуг от начала до конца. Этот принцип позволит отследить заявки клиентов и проинформировать их об этапах выполнения услуги, применяя технологии, основанные на использовании данных.

Также при предоставлении услуг может быть сформирована цепочка с участием сервисов или приложений третьих сторон для повышения результативности при обработке запроса клиента.

1.2. Государственная единая облачная платформа

Цифровой формой организации взаимодействия при предоставлении услуг должна являться платформа. Трансформация в платформу происходит на основе единых механизмов включения новых акторов для содействия в исполнении сложных услуг (суперсервисов). Реализация принципа «правительство, как платформа» является базовым для цифрового правительства.

Предполагается использование Гособлака с целью предоставления общих платформ для цифровых государственных услуг.

Государственная единая облачная платформа будет представлять собой портал «Гособлако», в состав которого войдут:

– административный интерфейс и реестр IaaS и SaaS решений и других облачных продуктов для госзаказчиков,
– программно-определяемое хранилище,
– гипервизоры,
– системы резервного копирования,
– программно-определяемая сеть,
– системы управления виртуализацией,
– оркестратор,
– билинговая система,
– service-desk.

Для эффективного решения задачи информатизации государственного управления предусмотрен перевод государственных и муниципальных информационных ресурсов на сервисную модель с применением облачных технологий. [3]

В дополнение к инфраструктуре Гособлака будет разработана платформа совместного использования (PaaS) для предоставления электронных услуг. Ее цель состоит в создании общегосударственной инфраструктуры разработки ИКТ-приложений.

Для большинства электронных услуг будут использоваться микросервисы. Это могут быть услуги идентификации и аутентификации, услуги уведомления с использованием сервисов службы коротких сообщений и др. Таким образом различные министерства и ведомства эффективно и быстро будут разрабатывать, и внедрять собственные электронные услуги и мобильные приложения. При этом им не нужно будет инвестировать средства в создание собственной инфраструктуры разработки электронных услуг, так как они смогут предоставлять услуги своим клиентам через платформу совместного использования.

Основными компонентами цифрового правительства являются единый портал, единые данные, государственная инфраструктура и межведомственные сервисы для совместного использования, сенсорные сети и аналитика, кибербезопасность и конфиденциальность.

СМЭВ

Сегодня информационные системы федеральных и муниципальных ведомств и организаций осуществляют взаимодействие между собой, а также с Единым порталом госуслуг согласно государственной целевой программе «Информационное общество (2011—2020 годы)», используя системы Межведомственного электронного документооборота (МЭДО) и единую систему межведомственного электронного взаимодействия (СМЭВ).

СМЭВ создана в соответствии с Федеральным законом Российской Федерации от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

СЭМВ обеспечивает предоставление государственных услуг и информационного взаимодействия в электронной форме для исполнения государственных функций, и реа-

лизации технологической возможности информационного взаимодействия участников: заявителей, региональных органов исполнительной власти, федеральных органов исполнительной власти, федеральных, региональных и муниципальных ведомств и др.

Заявители взаимодействуют с системой через Единый портал государственных и муниципальных услуг (ЕПГУ) или МФЦ.

СМЭВ выполняет следующие функции (табл. 1.1).

Таблица 1.1

Функции СМЭВ

Транспортные функции	Маршрутизация и доставка сообщений участников информационного обмена
Прикладные функции	Предоставление интерфейса веб-сервиса Реализация бизнес-логики услуги Форматно-логический контроль сообщений Формирование запросов и ответов в системе поставщик-потребитель
Общесистемные функции	Аутентификация и авторизация систем-потребителей Проверка сертификатов и электронных подписей систем — участников и пользователей Формирование идентификатора сообщения Формирование электронных подписей участников Преобразование форматов сообщений Публикация и хранение веб-сервисов Формирование системных сообщений-отказов для систем-участников Формирование задач с участием человека Ведение журнала действий участников Взаимодействие с удостоверяющим центром

Запрос и получение структурированной информации и электронных документов из информационных систем, взаимодействующих посредством СМЭВ, осуществляются с использованием программных средств веб-сервисов.

Сообщение СМЭВ имеет формат XML и содержит конверт; заголовок с ЭЦП, хеш; информацию об отправителе и получателе; блок, содержащий запрос/ответ.

Передача электронных сообщений ведется с использованием протокола SOAP.

Для электронного документооборота используется формат PDF/A, а реквизиты электронного документа размещаются в XML-файле.

Таблица 1.2

Функции СМЭВ

Транспортные функции	Маршрутизация и доставка сообщений участников информационного обмена
Прикладные функции	Предоставление интерфейса веб-сервиса Реализация бизнес-логики услуги Форматно-логический контроль сообщений Формирование запросов и ответов в системе поставщик-потребитель
Общесистемные функции	Аутентификация и авторизация систем-потребителей Проверка сертификатов и электронных подписей систем — участников и пользователей Формирование идентификатора сообщения Формирование электронных подписей участников Преобразование форматов сообщений Публикация и хранение веб-сервисов Формирование системных сообщений-отказов для систем-участников Формирование задач с участием человека Ведение журнала действий участников Взаимодействие с удостоверяющим центром

Сегодня для подключения к СМЭВ3 нужно отправить в Минкомсвязи заявку, получить электронную подпись, выполнить регистрацию информационной системы в тестовой среде, организацию защищенного канала связи, регистрацию информационной системы в продуктивной среде,

регистрацию услуги, регистрацию видов сведений (ВС), получить доступ к ВС в продуктивной среде.

СМЭВ разделена на два контура (рис. 1.3).

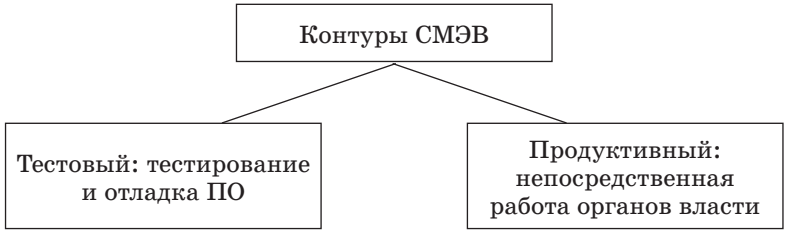


Рис. 1.3. Контуры СМЭВ

Тестовый контур доступен для подключения всех желающих из Интернета. Для упрощения разработки веб-сервисы должны в тестовом контуре иметь экземпляр. Продуктивный контур размещен в защищенной сети. В данном контуре веб-сервисы работают в полном объеме.

СМЭВ состоит из среды передачи данных, узлов сети СМЭВ, информационных систем поставщиков и потребителей информации, имеющих соответствующие веб-сервисы и адаптеры.

Среда передачи данных — защищенная сеть, которая имеет два сегмента — федеральный и региональный.

Она функционирует поверх протокола TCP с применением шифрования трафика, используя программные и аппаратные средства, имеющие сертификат ФСТЭК.

Сегодня структура СМЭВ состоит из 84 узлов, которые находятся на базе семи ЦОДов «Ростелекома» в разных частях России. Федеральными органами власти используется один узел, а остальные узлы — регионами.

В СМЭВ взаимодействие может осуществляться в синхронном и асинхронном режимах. Если для подготовки ответа на запрос требуется короткий временной интервал, используется синхронное взаимодействие, при котором в ответ на запрос информационная система поставщика отправляет результат в виде электронного сообщения.

В противном случае взаимодействие выполняется в асинхронном режиме, а поставщик в ответ отсылает специальное служебное сообщение («тикет») с указанием, что запрос принят, и с уникальным номером сообщения [4].

СМЭВ повышает эффективность работы органов федеральной и региональной власти. Институциональная основа СМЭВ может стать основой последующего развития системы, необходимого для функционирования цифрового правительства. При этом систему потребуется технологически усилить для совершенствования обмена сообщениями и осуществления транзакций в реальном времени, их обработки при взаимодействии с пользователями, бизнесом, с другими органами государственной власти.

МЭДО

В инфраструктуре единой системы электронного правительства важное место занимает Межведомственный электронный документооборот (МЭДО), предназначенный для обеспечения взаимодействия систем электронного документооборота его участников: Администрации Президента РФ, Аппарата Правительства РФ, а также федеральных органов государственной власти.

Положение о МЭДО было утверждено 22 сентября 2009 года.

«Межведомственный электронный документооборот представляет собой взаимодействие информационных систем электронного документооборота федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и иных государственных органов, а также организаций, созданных для выполнения задач, поставленных перед Правительством Российской Федерации, и организаций, созданных в целях осуществления предусмотренных законодательством Российской Федерации полномочий федеральных органов исполнительной власти». [5]

Взаимодействие электронного документооборота институтов власти подразумевает ведение электронной переписки, которая может содержать общедоступную информацию и сведения, составляющие служебную тайну.

Техническая инфраструктура МЭДО состоит из головного узла межведомственного документооборота, узлов участников МЭДО, защищенных каналов связи.

Взаимодействие в МЭДО осуществляется с помощью передачи сообщений, содержащих: файлы с документами; реквизиты документации в виде метаданных; информацию о состоянии документа, его принятии к исполнению, ходе рассмотрения и т. д.

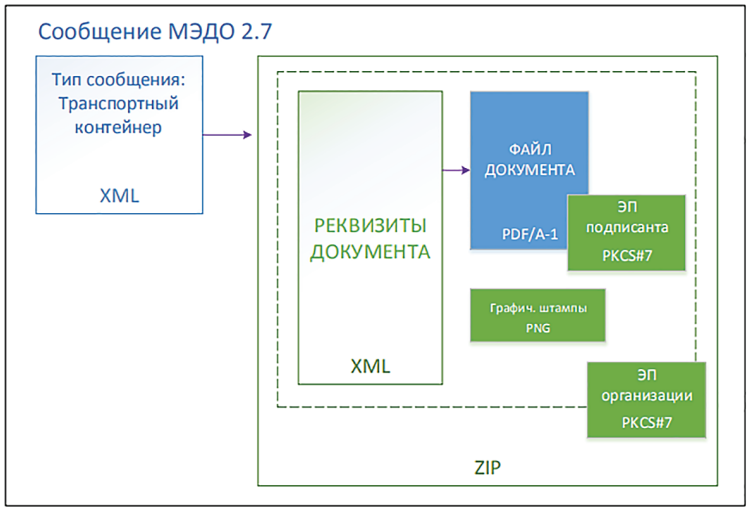


Рис. 1.4. Документ, подписанный ЭП, передаваемый в соответствии со схемой ЭСДМЭДО версии 2.7 [6]

Обмен и взаимодействие должны происходить в едином формате. Официальный формат обмена PDF/A. Все файлы объединяются в один zip-файл транспортного контейнера.

Порядок взаимодействия следующий:

– отправители в собственной системе электронного документооборота (СЭД) формируют документы, подписанные электронной подписью (подписями);

– отправители формируют регистрационные данные исходящего документа, их координаты и весь пакет отправляют получателю в виде сообщения для МЭДО.

– при получении документ и электронная подпись проверяются на соответствие государственным требованиям и, если проверка прошла успешно, данные регистрируются в собственной СЭД.

Для обеспечения качественного взаимодействия на рабочих местах предполагается наличие шлюзов с операционными системами, соответствующего серверного программного обеспечения, адаптерного блока, приводящего карточки СЭД-документации организации в унифицированный формат и т. д.

Чтобы стать участником МЭДО, потребуется получение адреса и идентификатора в ФСО РФ.

Участники взаимодействия должны обеспечить защиту информации, интеграцию в единые системы, автоматизацию, соответствие законодательным нормам и непрерывность обмена данными.

ЕСИА

Целью Единой системы идентификации и аутентификации (ФГИС ЕСИА), создаваемой Министерством связи и массовых коммуникаций Российской Федерации, является упорядочение и централизация процессов регистрации, идентификации, аутентификации и авторизации пользователей.

Пользователи системы — физические и юридические лица, а также органы государственной власти. При регистрации в системе осуществляется проверка значимых для удостоверения личности критериев.

Основные функциональные возможности ЕСИА представлены на рисунке 1.5.

Идентификация и аутентификация пользователей	Поддержка различных методов аутентификации Однократная аутентификация Поддержка уровней достоверности идентификации пользователя
Ведение идентификационных данных	Ведение регистров физических лиц Ведение регистров юридических лиц Ведение регистров органов и организаций Ведение регистров должностных лиц Ведение регистров информационных систем
Авторизация уполномоченных лиц органов государственной власти при доступе к возможностям:	Ведение регистра должностных лиц органов власти и ЕСИА Ведение справочника полномочий в отношении информационной системы и предоставление пользователям ЕСИА полномочий по доступу к ресурсам систем, зарегистрированным в ней Делегирование полномочий уполномоченным лицам нижестоящих органов государственной власти
Ведение и предоставление информации о полномочиях пользователей в отношении информационных систем, зарегистрированных в ЕСИА	

Рис. 1.5. Основные функциональные возможности ЕСИА

Сегодня подключиться к ЕСИА могут государственные и некоторые коммерческие организации: страховые компании, банки, финансовые организации, операторы связи и др.

ЕПГУ

Единый портал государственных и муниципальных услуг (ЕПГУ) запущен в 2009 году. На нем размещается информация, формы заявок и проводятся платежи.

Оператором Единого портала является Министерство связи и массовых коммуникаций Российской Федерации.

ЕПГУ интегрирован с Единой системой идентификации и аутентификации (ЕСИА) в 2015 году. При дальнейшем развитии системы это может стать хорошим фундаментом.

ЕПГУ — государственная информационная система, обеспечивающая доступ физических и юридических лиц к информации обо всех видах услуг; для предоставления услуг в электронной форме; для рассмотрения обращений граждан и учета мнения граждан о качестве и доступности услуг.

На ЕПГУ приведено описание услуг, оказываемых федеральными, региональными органами власти РФ, органами местного самоуправления.

Это услуги в сфере образования, здравоохранения, культуры, жилищно-коммунального хозяйства, имущественно-земельных отношений, строительства и регулирования предпринимательской деятельности, социальной защиты населения.

В личном кабинете можно формировать запросы на предоставление услуг, получать доступ к различным электронным сервисам органов государственной и муниципальной власти, ответы на обращения, отслеживать стадии исполнения запрошенной услуги.

Также в личном кабинете представлены результаты анализа индивидуального профиля, информация об истории заказанных услуг, платежей и операций. Есть возможность настройки уведомлений. Услуги соотнесены с конкретными субъектами РФ, поэтому от пользователя сначала требуется выбрать регион, затем услуги, предоставляемые на его территории. Основная цель личного кабинета — предоставление персонифицированных услуг. Интерфейс портала совершенствуется для того, чтобы индивидуализировать сервисы и перейти к обслуживанию пользователей портала по жизненным ситуациям.

ЕПГУ предоставляет единый пользовательский интерфейс, Единый личный кабинет, каталог услуг, сер-

висы навигации и поиска, Единую систему идентификации и аутентификации, информационно-платежный шлюз, сервис досудебного обжалования, единый сервис поддержки пользователей.

ЕБС

Разработчиком и оператором Единой биометрической системы (ЕБС) является «Ростелеком». Система работает во взаимодействии с Единой системой идентификации и аутентификации (ЕСИА), которая хранит персональные данные граждан.

ЕБС хранит только биометрические данные граждан в обезличенной форме в виде математической модели без привязки биометрических данных к данным их владельца. Для связи с ЕСИА с целью подтверждения образца используется технологический идентификатор — набор цифр.

ЕБС предназначена для оказания дистанционных услуг. Для удаленного открытия банковского счета необходимо, в первую очередь, создать учетную запись в ЕСИА и пройти регистрацию в Единой биометрической системе по записи голоса и фотографии.

При разработке ЕБС были использованы технологии нейросетей, поведенческой биометрии, работы с большими данными. Модуль lifeness в процессе распознавания биометрического образца обеспечивает проверку присутствия перед монитором живого человека, а не фотографии.

В модуле аномалий на основе работы математического аппарата с большими данными реализовано взаимодействие с системой геолокации, определение типа мобильного устройства, веб-интерфейса, количества запросов в единицу времени, количества ошибок, при вводе логина-пароля или сдаче биометрии, количества запросов за предыдущий период времени. Такие данные являются основой предиктивной аналитики с вероятностным предсказанием аномалий для распознавания попыток обойти систему.

Биометрическая платформа имеет открытую архитектуру и является муливендорной. С ней работают такие известные компании, как ЦРТ, VisionLabs (платформа LUNA), NtechLab, ФГУП ГосНИИАС, «АСМ Решения», «Вокорд», МИФИ, МФТИ и др.

Для определения качества программных продуктов компания совместно с Русским биометрическим обществом, Минсвязи и ФСБ разработала специальные стандарты и требования.

С помощью ЕБС сегодня уже можно открыть счет/вклад/депозит, оформить заявку на кредит и денежный перевод.

Система будет развиваться и масштабироваться на другие финансовые услуги и сектора экономики.

Банк России планирует расширить применение ЕБС в таких направлениях, как страхование, госуслуги, получение облачной квалифицированной электронной подписи, медицинские услуги и др.

Чтобы попробовать биометрическую систему в действии, необходимо:

– выбрать интересующую услугу на сайте банка или в мобильном приложении,

– авторизоваться в ЕСИА,

– пройти биометрическую идентификацию (для этого открыть отдельное мобильное или браузерное приложение), отправив видеозапись произношения случайно выведенных на экран цифр,

– ЕБС сверяет биометрические идентификационные данные с эталонным образцом,

– при успешной идентификации в банк, оказывающий услугу, отправляются персональные данные клиента из ЕСИА.

ЕГИССО

Единая государственная информационная система социального обеспечения (ЕГИССО) разрабатывается с целями:

– совершенствования качества предоставляемых гражданам в области социальной сферы услуг;

– проактивного предоставления мер социальной защиты;

– получения госорганами сведений для предоставления мер социальной защиты;

– прогнозирования социальных расходов бюджетной системы с использованием систем аналитики;

– предоставления населению информации о мерах социальной защиты и правах на нее;

– адресного предоставления мер социальной защиты с учетом нуждаемости в них.

В рамках этой системы внедряется проактивное предоставление мер социальной поддержки, когда на основании данных информационная система при наступлении определенного события самостоятельно предлагает гражданину меры социальной поддержки, с которыми остается только согласиться.

Для автоматизированного информирования граждан будут использоваться: личный кабинет единого портала государственных услуг; электронная почта; SMS-сообщение; телефонный звонок.

Цифровая трансформация

Согласно прогнозам Gartner на смену электронному правительству (e-government) неизбежно приходит цифровое правительство (digital government), при котором одним из ключевых моментов будет прозрачность управления. [7]

В результате дальнейшей интеграции и совершенствования информационных систем различных ведомств будет построена единая цифровая платформа.

Реализация федерального проекта «Цифровое государственное управление» позволит осуществить окончательный переход на электронное взаимодействие граждан и организаций с государством. В частности, будет реализована реестровая модель, экстерриториальность

и проактивность при предоставлении государственных и муниципальных услуг в электронной форме, сформированы механизмы обратной связи с гражданами и организациями, юридически значимый документооборот станет по преимуществу электронным.

«Среди ключевых показателей, которые планируется достигнуть к 2024 году:

– государственные (муниципальные) услуги предоставляются проактивно и онлайн, действуют 25 цифровых «супер-сервисов» по жизненным ситуациям;

– 90% внутри- и межведомственного юридически значимого электронного документооборота государственных и муниципальных органов и бюджетных учреждений автоматизировано;

– 60% граждан имеют цифровое удостоверение личности с квалифицированной электронной подписью». [8]

1.3. Модели и платформы предоставления государственных услуг

Реестровая модель предоставления государственных услуг

Сегодня активно внедряется «реестровая модель» предоставления государственных услуг, при которой результатом является не бумажный документ, а запись в электронном реестре. Отдельным сервисом может являться получение выписки из этого реестра. «Реестровая модель» предусматривает хранение результатов услуг государственных информационных ресурсов и предоставление выписки из них по требованию заявителя. Модель уже используется в Росреестре, ФНС России, Росаккредитации и ряде других ведомств.

Ее использование позволяет:

– снизить расходы на содержание персонала и изготовление материальных носителей для создания результата услуги;

– исключить возможности подделки документов на материальном носителе.

Межведомственная платформа юридически значимого электронного документооборота (ЮЗЭДО)

ЮЗЭДО — Юридически значимый электронный документооборот.

Согласно ГОСТ Р 7.0.8—2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения», юридическая значимость документа — это свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера. В Федеральном законе № 63-ФЗ «Об электронной подписи» определяется, что для юридической значимости документ должен обладать простой электронной или усиленной квалифицированной электронной подписью. (Статья 5, п. 1 Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» (с изм. и доп., вступ. в силу с 31.12.2017)).

Типичными электронными документами ЮЗЭДО являются: договоры, акты, накладные, универсальные передаточные документы и т. д.

Обычно организации используют усиленную электронную подпись для обмена документами. Такая подпись имеет ключи проверки и сертификаты уникальности, защищая документ от подделки, внесения изменений и контролируя его целостность. С использованием технологий ЮЗЭДО можно обеспечить усиленный контроль за движением документов, так как они будут проходить через единую систему электронного документооборота и фиксироваться в ней. Появится возможность проследить движение документов, статус их обработки. При этом документ нельзя будет потерять, удалить или пропустить.

Платформа ЮЗДО

Целевая функциональная структура «ГИС Платформа ЮЗЭДО» была представлена ФГБУ НИИ «Восход» на конференции компании «Электронные офисные систем» (ЭОС).

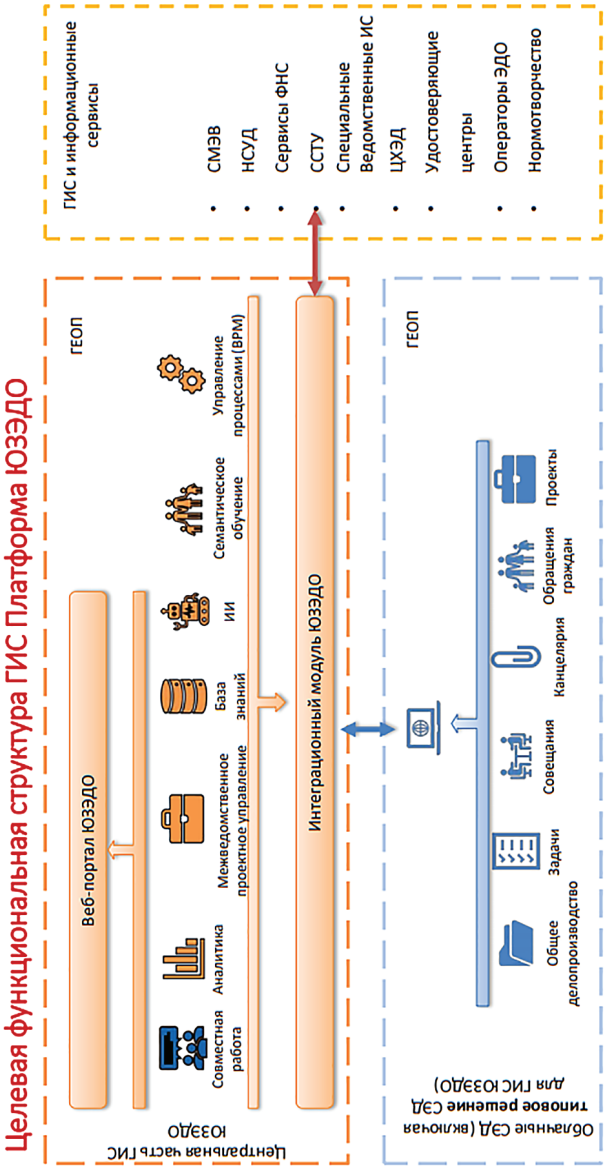


Рис. 1.6. Целевая функциональная структура ГИС Платформа ЮЗЭДО [6]

Результатом внедрения платформы являются: «обеспечение прозрачности межведомственных процессов, автоматизация обработки обращений граждан с предварительной подготовкой ответов, совместная работа над документами, получение показателей эффективности процессов и сотрудников, загрузка в систему нормативных актов в машиночитаемом виде с планом проекта, процессами, электронными формами, распределением ролей и т. д., автоматизированные предложения по оптимизации процессов, выявление аномалий в работе сотрудников».

Электронные документы могут быть приняты на государственное хранение электронных документов из систем электронного документооборота органов государственной власти в Центр хранения электронных документов (ЦХЭД).

ЦХЭД также предназначен для оказания государственных услуг в сфере обеспечения архивной информацией органы исполнительной власти, организаций и граждан.

Цифровое хранилище электронных документов (ЦХЭД) является программно-техническим комплексом, обеспечивающим физическое размещение, сохранность и защищенный доступ к оригиналам электронных документов, заверенных электронной подписью.

1.4. Мобильная и облачная электронные цифровые подписи

Мобильная электронная цифровая подпись (ЭЦП) — технология, которая позволяет использовать мобильный телефон в качестве надежного средства идентификации при получении электронных сервисов.

Личный ключ мобильной ЭЦП хранится на sim-карте мобильного телефона, смартфона или планшета с поддержкой функции ЭЦП, поэтому документ может быть подписан в любое время и в любом месте. Установленное на sim-карте приложение осуществляет привязку сертификата ЭЦП. При получении пользователем такого устройства электронного документа, который необходимо подписать ЭЦП, он может подтвердить визирование вводом PIN-кода. Система имеет еще несколько дополнительных возможностей — таких как авторизация в информационных системах, идентификация с целью получения цифровых услуг. На российском рынке технологию мобильной цифровой подписи первым предложила компания «Мегафон».

«Облачная» квалифицированная электронная подпись — это юридически значимая электронная подпись, реализованная с помощью технологии, позволяющей перенести на облачный сервер — в «облако» — все вычислительные операции, связанные с применением электронной цифровой подписи.

Вариантами аутентификации пользователей облачной квалифицированной электронной подписи могут быть: мобильное приложение myDSS, SIM-карта с криптографическим апплетом.

Хранилище ключей — КриптоПро HSM, снабжено датчиками вскрытия, механизмами доверенной генерации и уничтожения ключей, «барьером» от утечек по побочным каналам и от внутреннего нарушителя (администратора), а также другими уровнями защиты. Ключи становятся неизвлекаемыми и некомпрометируемыми.

Облачная цифровая подпись позволяет вести документооборот в любом уголке мира, независимо от устройства. Страны европейского союза активно занимаются оформлением особо важных документов через «облако». Возможность удобного и надежного хранения данных на облачном сервере в настоящее время имеют и граждане Российской Федерации.

Цифровой профиль

Цифровой профиль — это совокупность цифровых записей о физических и юридических лицах, содержащихся в государственных информационных системах, предоставление которых обеспечивается с использованием

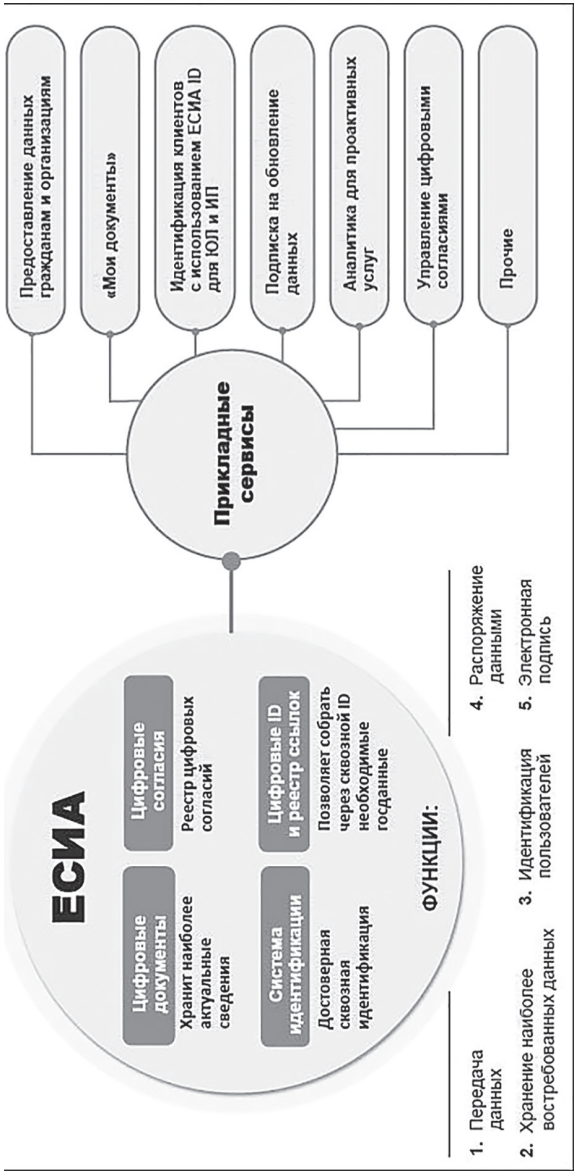


Рис. 1.6. Сервисы цифрового профиля [10]

технологической инфраструктуры, которая позволяет использовать данные пользователя с согласия, предоставляемого в цифровом виде.

Создание инфраструктуры цифрового профиля будет осуществляться на основе единой системы идентификации и аутентификации. Для наполнения цифрового профиля сведениями будут использоваться имеющиеся государственные и муниципальные информационные системы.

Инфраструктура цифрового профиля создаст возможность автоматизированного получения данных о гражданах посредством «единого окна».

В число сервисов цифрового профиля, как это видят в Минкомсвязи, войдёт хранение актуальных сведений, прикладные сервисы, а также реестр цифровых согласий.

Инфраструктура Цифрового профиля должна обеспечить доступность к данным, обмен сведениями из государственных информационных систем о гражданах и функционирование платформы управления согласиями на доступ к данным.

«Государство-как-Платформа»

Идея государства как платформы, сформулированная Центром стратегических разработок в 2016 г., — «Государство-как-Платформа» — это цифровая экосистема из трех основных групп — субъектов взаимоотношений при социально-экономическом развитии страны: государство, граждане, бизнес.

«Государство перейдет от предоставления единичных “точечных” сервисов при помощи государственных (ведомственных) информационных систем (ГИС) и баз данных к комплексному решению жизненных ситуаций человека.

Человек, идентифицируясь в государственной платформе, с помощью своего «цифрового двойника» будет взаимодействовать с цифровой экосистемой и получать от нее цифровые сервисы в соответствии со своими потребностями». [11]

Технологии платформы: интернет вещей, облачные технологии, распределенный реестр, искусственный интеллект, большие данные, единая система цифрового доверия.

Предусматривается введение единой фронтальной системы с омниканальностью (включая чат-бот), экосистемы микросервисов, использование эталонных данных в единой метамодели данных, перевод всех востребованных услуг в электронную форму. А также использование ключевых общих информационных ресурсов, максимальной «облачности» сервисов, «цифровых двойников», цифрового профиля, цифровой подписи на основе единой системы идентификации, проактивного предоставления интегрированных услуг, решений, принимаемых системами искусственного интеллекта.

Вопросы для самоконтроля

1. Основные области для реализации инициатив электронного правительства.
2. Состав электронного правительства.
3. Развитие электронного правительства в других странах.
4. Основные элементы цифрового правительства.
5. Межведомственная платформа юридически значимого электронного документооборота (ЮЗЭДО).
6. ЕПГУ и ЕБС.
7. Система межведомственного электронного документооборота.
8. Единая система межведомственного электронного взаимодействия.
9. Цифровой профиль физического и юридического лица.

Список использованных источников главы 1

1. Arild Jansen. Assessing E-government progress — why and what. Department of e-government studies, University of Oslo. Norway. — URL: https://www.jus.uio.no/ifp/om/organisasjon/afin/forskning/notatserien/2005/7_05.pdf

2. Цифровое правительство 2020. Перспективы для России: Доклад сотрудников Всемирного банка совместно с Институтом развития информационного общества. Апрель 2016 г. — URL: http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf

3. Распоряжение Правительства РФ от 28 августа 2019 г. № 1911-р. «Об утверждении концепции создания государственной единой облачной платформы». — URL: https://rulaws.ru/goverment/Rasporyazhenie-Pravitelstva-RF-ot-28.08.2019-N-1911-r/

4. Система Межведомственного электронного взаимодействия. Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии. Версия 2.4.4. — URL: https://smev.gosuslugi.ru/portal/

5. Положение о системе межведомственного электронного документооборота от 22 сентября 2009 года № 754 (с изменениями на 16 марта 2019 года). — URL: http://docs.cntd.ru/document/902176142

6. Методические рекомендации по реализации Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде. — URL: https://digital.gov.ru/uploaded/files/metodicheskie-rekomendatsii-558pr.pdf

7. Gartner: Государство и бизнес движутся к цифровой эре // Журнал ПЛАС. — 23 мая 2017. 18:34. — URL: https://www.plusworld.ru/journal/section_1817/plus-4—2017/gartner-gosudarstvo-i-biznes-dvizhutsya-k-tsifrovoj-ere/

8. Паспорт федерального проекта «Цифровое государственное управление». Последнее обновление: 22 октября 2019. — URL: https://digital.gov.ru/ru/activity/directions/882/

9. Презентация «Платформа юридически значимого электронного документооборота (ЮЗЭДО). Подход к созданию и эксплуатации» / Руководитель проектов Гортинский Сергей. — URL: https://www.eos.ru/upload/od2019/Gortinskii_UZEDO.pdf

10. Цифровой профиль гражданина — что известно на сегодняшний день / Татьяна Костылева. — 27.03.2019. — D-Russia.ru. — URL: http://d-russia.ru/tsifrovoj-profil-grazhdanina-chto-izvestno-na-segodnyashnij-den.html

11. Государство как платформа / Михаил Петров, Василий Буров, Мария Шклярук, Андрей Шаров. — Центр стратегических разработок. — Апрель 2018. — URL: https://www.csr.ru/wp-content/uploads/2018/05/GOSUDARSTVO-KAK-PLATFORMA_internet.pdf

Глава 2
ПОСТРОЕНИЕ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА И ОРГАНИЗАЦИИ ДЛЯ РАЗВИТИЯ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ И КОММЕРЧЕСКИХ УСЛУГ

Концепция и архитектура цифрового профиля разрабатывается в рамках Плана мероприятий по направлению «Информационная инфраструктура» Программы «Цифровая экономика Российской Федерации» [1], принятой в соответствии с Указом Президента России 7 мая 2018 года №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [2] и утвержденной 24 декабря 2018 года на заседании президиума Совета при Президенте России по стратегическому развитию и национальным проектам.

Введение цифрового профиля в промышленную эксплуатацию планируется к концу сентября 2020 года.

2.1. Понятие, цели и принципы создания цифрового профиля

Цифровизация экономики формирует большие массивы данных у всех участников информационного обмена, первоисточники которых содержатся в государственных информационных системах (ГИС) и необходимы для осуществления как государственных функций, так и оказания услуг гражданам. Совокупность таких данных формирует Цифровой профиль гражданина и организации.

Цифровой профиль гражданина — это совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций.

Системы Цифрового профиля составляют технологическую инфраструктуру, которая позволяет использовать данные гражданина из Цифрового профиля (включая данные в ГИС, доступные по ссылкам) с его согласия, предоставляемого в цифровом виде.

Основные характеристики Цифрового профиля гражданина показаны на рис. 2.1.

Рис. 2.1. Основные характеристики инфраструктуры Цифрового профиля гражданина

Цифровой профиль организации является совокупностью цифровых записей об организации, которые содержатся в информационных системах государственных органов и организаций.

Системы Цифрового профиля составляют технологическую инфраструктуру, которая позволяет использовать данные юридического лица с его согласия, предоставляемого в цифровом виде.

Цифровой профиль юридического лица строится на основе ОГРН и ОГРНИП — основного государственного регистрационного номера юридического лица (индивидуального предпринимателя).

ОГРН (ОГРНИП) присваивается регистрирующим органом при внесении первой записи в ЕГРЮЛ (ЕГРИП).

Данные Цифрового профиля юридического лица содержатся в Едином государственном реестре юридических лиц (ЕГРЮЛ) и Едином государственном реестре индивидуальных предпринимателей (ЕГРИП), иных государственных системах и реестрах.

Руководитель юридического лица за счет связки Цифрового профиля юридического лица и физического лица имеет возможность поручить (делегировать) другому уполномоченному лицу проведение определённых операций в цифровом виде. Такое делегирование руководитель юридического лица выполняет в Цифровом профиле юридического лица с использованием квалифицированной электронной подписи и фиксирует в реестре цифровых согласий юридического лица, который фактически также является реестром полномочий.

Существующие в настоящее время механизмы доступа к государственным данным имеют недостатки, препятствующие эффективному цифровому взаимодействию, в том числе:

– отсутствие формализованных механизмов обработки данных с целью повышения уровня и качества жизни граждан;

– недостаточный уровень доступности, качества и актуальности государственных данных, необходимых для перехода на цифровое взаимодействие;

– отсутствие инфраструктуры, способной обеспечить унифицированный, безопасный, быстрый и удобный обмен данными между всеми участниками;

– отсутствие стандартов и решений в сфере информационной безопасности, в том числе криптографии, для обеспечения безопасного обмена данными между государственными органами и коммерческими компаниями;

– отсутствие соответствующей нормативно-правовой базы.

Наличие вышеуказанных барьеров приводит к возникновению следующих негативных последствий для организаций и граждан:

– высокий уровень операционных расходов, связанных с обработкой бумажных документов, необходимостью личного присутствия физического лица, ручной проверки и подтверждения предоставленных данных;

– низкая эффективность внутренних бизнес-процессов организаций, связанных с аналитикой данных (скоринг, риск-менеджмент, оценка просроченной задолженности, подготовка отчетности и т. д.);

– низкое качество клиентского опыта, снижение конверсии, недоступность части услуг для отдельных групп клиентов (например, услуг, требующих личного присутствия (подача документов, идентификация), для граждан, проживающих в труднодоступных регионах);

– сложность персонализации продуктов и услуг на основе данных о физическом лице, полученных или актуализированных из внешних источников;

– отсутствие у гражданина возможности управления выданными согласиями в электронном виде.

Создание инфраструктуры «Цифровой профиль» позволит устранить эти барьеры и создаст возможность автоматизированного получения данных о гражданах и организациях посредством «единого окна».

Целями создания Цифрового профиля являются:

– обеспечение возможности для граждан управления передачей и обработкой своих данных (управление цифровыми согласиями), содержащихся в Цифровом профиле;

– обеспечение возможности использования с согласия гражданина данных, содержащихся в Цифровом профиле, организациями в целях предоставления различных услуг;

– обеспечение удобного, прозрачного и безопасного обмена данными между участниками информационного обмена;

– повышение доверия между участниками обмена данными;

– обеспечение оперативного и безопасного получения данных из государственных информационных систем;

– развитие цифровых финансовых, государственных и иных услуг.

Цифровой профиль может использоваться:

1. Для идентификации. Цифровой профиль хранит наиболее востребованные данные, а также ссылки на достоверные и юридически значимые данные, содержащиеся в государственных информационных системах, на основании которых органы власти и организации в соответствии с требованиями законодательства Российской Федерации могут провести дистанционную идентификацию без необходимости предоставления клиентом бумажных документов.

2. Для развития цифровых услуг, предоставляемых гражданам и организациям. Получение и обновление данных о клиенте (физическом или юридическом лице) коммерческими организациями позволит на основеданной информации, доступной в режиме онлайн, развивать цифровые услуги для граждан, что будет способствовать развитию цифровой экономики в целом.

В первую очередь такими коммерческими организациями являются:

– финансовые организации, которые должны с установленной законом периодичностью актуализировать персональные данные клиентов;

– негосударственные пенсионные фонды и страховые компании, оказывающие услуги управления средствами пенсионных накоплений и страхования;

– профессиональные участники рынка ценных бумаг, осуществляющие ведение реестра владельцев ценных бумаг;

– удостоверяющие центры, формирующие и выдающие гражданину сертификат ключа проверки электронной подписи;

– операторы связи и телекоммуникационные компании, предоставляющие услуги связи;

– прочие компании — провайдеры услуг и сервисов, для оказания которых требуется идентификация гражданина.

3. Для предоставления комплексных государственных услуг. Получение государственных и муниципальных услуг часто связано с жизненными ситуациями граждан, в которых они не обладают достаточной информацией о своих правах и порядке получения полагающихся им услуг. Инфраструктура Цифрового профиля позволит перейти на проактивную модель предоставления государственных и муниципальных услуг. Например, в случае заказа заграничного паспорта и при истечении срока его действия Цифровой профиль напомнит заявителю о необходимости заблаговременной замены паспорта и позволит заполнить заявление о его замене в «один клик».

Цифровой профиль поможет выявить наиболее значимые ситуации, происходящие в жизни гражданина, разрешение которых требует неоднократного обращения в различные государственные органы и организации. Такой подход приведет к повышению доступности государственных и муниципальных услуг в электронном виде, осведомленности об этом граждан и их удовлетворенности.

Цифровой профиль может применяться в следующих случаях:

– для получения государственных и муниципальных услуг;

– при взаимодействии с различными коммерческими организациями (банками, микрофинансовыми организациями, НПФ, страховыми компаниями, операторами связи и иными) для получения услуг;

– для актуализации данных о своих клиентах коммерческими организациями на основе источника достоверных и юридически значимых данных.

Взаимодействие участников инфраструктуры Цифрового профиля будет построено на принципах доверия между всеми участниками процесса обработки данных и обеспечит для них ряд преимуществ.

Для граждан:

– повышение доступности услуг за счет их предоставления полностью в цифровом виде;

– снижение стоимости услуг за счет цифровизации и оптимизации процессов их предоставления;

– сокращение времени и количества шагов для получения услуг в цифровом виде;

– управление своими данными в режиме 365/7/24;

– повышение цифровой грамотности.

Для государства:

– повышение эффективности государственных управленческих решений за счет увеличения объема данных, обрабатываемых в автоматизированном виде;

– перевод ГИС на реестровую модель формирования, ведения и предоставления данных, а также обеспечение юридической значимости соответствующих записей в реестрах;

– возможность использования государственными органами данных полностью в цифровом виде, в том числе в целях предоставления государственных услуг;

– возможность использования государственными органами цифровых технологий для снижения регуляторной нагрузки на организации;

– исключение дублирования данных (дедупликация) в разных информационных ресурсах, кроме дублирования наиболее востребованных видов сведений с целью снижения нагрузки на каналы передачи данных;

– повышение безопасности при обмене данными;

– развитие ГИС и снижение на них нагрузки.

Для организаций:

– повышение операционной эффективности за счет увеличения объема данных, используемых при принятии управленческих решений;

– «единое окно» для получения данных из ГИС;

– повышение качества, доступности и скорости предоставления данных;

– сокращение времени и количества шагов для открытия и ведения бизнеса («в один клик»);

– появление новых сервисов и бизнес-моделей, основанных на обработке и анализе данных;

– получение согласия на передачу и обработку персональных данных в цифровом виде.

Таким образом, Цифровой профиль будет напрямую способствовать переходу от модели запроса «точечных» услуг к модели предоставления государственными органами и организациями для граждан и организаций комплексных продуктов и услуг в зависимости от их жизненной ситуации.

Основными принципами создания инфраструктуры Цифрового профиля являются следующие:

– физическое лицо вправе свободно распоряжаться доступом к своим данным, хранящимся в различных государственных информационных системах;

– использование и передача данных из Цифрового профиля физического лица происходит только с его согласия; если передача данных не предусмотрена законодательством Российской Федерации; физическое лицо управляет процессом предоставления и отзыва согласия;

– для предоставления цифрового согласия на доступ к данным из своего Цифрового профиля гражданин должен пройти идентификацию и аутентификацию с использованием простой или квалифицированной электронной подписи;

– наиболее востребованные данные, такие как цифровые копии документов, будут храниться в Цифровом профиле, при этом остальные данные хранятся в информационных системах, в которых они первоначально создаются;

– доступ к данным осуществляется напрямую из Цифрового профиля в случае, если такие данные хранятся в информационных системах Цифрового профиля, либо по ссылкам на источники данных с использованием идентификаторов, присваиваемых в соответствующих информационных системах;

– ответственность операторов персональных данных при обработке персональных данных с использованием инфраструктуры Цифрового профиля устанавливается в соответствии с законодательством Российской Федерации;

– связывание множества идентификаторов в различных информационных системах обеспечивает технологический идентификатор ЕСИА — ЕСИАID;

– обмен данными происходит в доверительной защищенной среде и способствует снижению операционных издержек государственных органов и коммерческих организаций, связанных со сбором, подтверждением и актуализацией таких данных.

– подключение коммерческих организаций к инфраструктуре Цифрового профиля осуществляется на добровольной основе, если иное не предусмотрено законодательством Российской Федерации.

Реализация ссылочной структуры Цифрового профиля возможна при условии перехода государственных органов — поставщиков данных на реестровую модель.

В целях повышения качества услуг в электронном виде, а также сокращения сроков их предоставления необходимо реализовать поэтапный переход к «полностью цифровым» услугам — так называемой «Реестровой модели» оказания государственных и муниципальных услуг, подразумевающей предоставление результата в виде внесения сведений в ГИС без выдачи результата на бумажном носителе.

В данном случае результатом оказания услуги будет являться запись в информационной системе (реестре) соответствующего государственного органа либо ее обновление с сохранением историитаких изменений. Реестровая модель предусматривает хранение результатов услуг в соответствующей ГИС и предоставление выписки из соответствующего реестра по требованию пользователя.

Для перехода государственных органов и организаций на реестровую модель необходимо:

– определить состав данных, который будет формировать Цифровой профиль, и поставщиков этих данных («золотая» запись);

– обеспечить возможность актуализации данных в ГИС, в которых они не создаются;

– определить перечень государственных и иныхуслуг и/или сведений, в результате получения которых будут накапливаться ссылки на данные в Цифровом профиле;

– обеспечить изменение законодательства, на основании которого предоставляются соответствующие услуги, для их перевода на реестровую модель — придание юридической значимости реестровой записи, замена бумажного документа на электронную выписку из государственного реестра;

– реализовать доработку соответствующих информационных систем государственных органов и организаций.

Введение реестровой модели является длительным процессом, который будет сопровождаться поэтапным переходом к внесению сведений в ГИС без выдачи результата на бумажном носителе. Для беспрепятственного обеспечения такого перехода необходимо урегулировать вопрос постоянного и временного архивного хранения документов, которые были сформированы до введения реестровой модели в электронном виде, определить перечень форматов и процедур их конвертации.

Кроме того, для использования реестровой модели в целях предоставления гражданам цифровых коммерческих услуг (например, финансовых) потребуется снятие ограничений в отраслевых законах. Так, за счет внедряемой модели электронного паспорта транспортного средства электронный полис ОСАГО, согласно нормам Федерального закона от 25 апреля 2002 г. № 40-ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных редств» [3], позволяет исключить из оборота бумажный вид полиса и использовать реестровый номер полиса как при проверке сотрудниками ГИБДД, так и при наступлении страхового случая, при этом реестровая запись с учетом всех необходимых данных о полисе хранится в информационной системе Российского союза автостраховщиков.

2.2. IT-архитектура и механизм работы цифрового профиля

Инфраструктура Цифрового профиля является единым источником доступа к юридически значимым данным, актуальность которых обеспечена за счет автоматического обновления данных из ведомственных информационных систем, а также ссылочного механизма на первичные источники данных. Потребители данных (государственные органы и организации, граждане, коммерческие организации, в том числе технологические стартапы) самостоятельно могут запросить данные с использованием инфраструктуры Цифрового профиля и с согласия владельца на их предоставление.

Участниками нформационного взаимодействия обеспечивается равноправный доступ к инфраструктуре Цифрового профиля.

Архитектура Цифрового профиля представлена на рис. 2.2.

Инфраструктура Цифрового профиля состоит из совокупности следующих элементов Единой системы идентификации и аутентификации (ЕСИА):

- система идентификации;
- система цифровых документов;
- система идентификаторов и реестр ссылок;
- система цифровых согласий.

Система идентификации позволяет физическим лицам управлять своими данными только после идентификации, которая может быть осуществлена с использованием ЕСИА, а в случаях, установленных в законе, с использованием ЕСИА и Единой биометрической системы (ЕБС).

Кроме того, при развитии инфраструктуры Цифрового профиля могу тприменяться иные способы идентификации в соответствии с законодательством Российской Федерации.

Основной задачей является обеспечение сервиса достоверной сквозной идентификации, позволяющей использовать государственные системы идентификации для доступа к управлению пользователями своими данными.

Рис. 2.2. Архитектура цифрового профиля

Инфраструктура Цифрового профиля будет также содержать систему цифровых документов, в которой будет обеспечиваться хранение и актуализация наиболее востребованных юридически значимых сведений.

Указанные сведения могут использоваться потребителями данных напрямую из цифрового профиля без запросов к ГИС, что позволит сократить нагрузку на канал обмена данными и увеличить скорость обмена данными.

Указанные данные будут храниться в ЕСИА, а их достоверность будет гарантироваться источниками, из которых они будут получены.

Кроме того, Инфраструктура цифрового профиля позволит предоставлять и сохранять документы и сведения в приложении на пользовательском устройстве и предоставлять доступ к ним в offline-режиме.

Система цифровых документов может хранить данные, получаемые из реестров ГИС. Полный состав сведений настраивается на этапе эксплуатации и доступен для дальнейшего изменения. При этом гражданин по желанию может дополнить состав сведений, которые размещаются в его цифровых документах, ограниченным списком сведений.

В рамках системы идентификаторов и реестра ссылок инфраструктура Цифрового профиля обеспечивает хранение реестра ссылок на источники данных, которые хранятся в соответствующих ГИС.

Для определения информационной системы, в которой содержатся данные, предусматривается создание системы идентификаторов и реестра ссылок.

Основной задачей является связывание всех идентификаторов владельца данных с использованием внутреннего идентификатора ЕСИА (ЕСИА ID).

При взаимодействии с ГИС используются «нативные» для такой системы идентификаторы сведений, которы есвязаны с ними через внутренний идентификатор ЕСИА.

Связывание различных идентификаторов друг с другом через внутренний идентификатор ЕСИА позволяет

получать любые виды данных по имеющемуся у организации идентификатору без внесения дополнительных сведений в ГИС и их доработки. Однако в случае готовности ГИС или создания новых информационных систем, внутренний идентификатор ЕСИА может использоваться в них как «нативный».

Реестр идентификаторов хранит в себе ссылки на записи в реестрах, содержащихся в ГИС, а также идентификаторы, использующиеся в них и связанные посредством ЕСИА ID.

Цифровое согласие является юридически значимой реестровой записью о предоставлении (отзыве) прав на сбор, передачу и использование данных в соответствии с указанной целью обработки. Все действия владельца данных с цифровыми согласиями (при предоставлении данных с использованием инфраструктуры цифрового профиля) будут отражаться в едином реестре цифровых согласий и доступны в личном кабинете пользователя.

Основной задачей является обеспечение хранения всех согласий, предоставленных владельцем данных при использовании инфраструктуры Цифрового профиля, в едином реестре, а также предоставление доступа к управлению своими цифровыми согласиями.

Цифровые согласия могут классифицироваться по сроку действия на разовые, когда согласие предоставляется на однократное предоставление сведений, и долгосрочные, когда гражданин дает право на многократное предоставление сведений на определенный срок.

Предоставление согласия на получение и обработку данных может также осуществляться с использованием действующего механизма «черновиков» в рамках получения третьей стороной запрашиваемых данных, в том числе с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации (ПЭП ЕСИА).

Цифровое согласие физическими лицами может быть подписано усиленной квалифицированной электронной подписьюили ПЭП ЕСИА, а в отдельных установленных законодательно случаях после проведения биометрической идентификации с использованием единой биометрической системы. Для юридических лиц и индивидуальных предпринимателей согласие предоставляется с помощью квалифицированной электронной подписи, в том числе облачной квалифицированной электронной подписью, или ПЭП ЕСИА после проведения биометрической идентификации с использованием единой биометрической системы.

При изменении законодательства в области электронной подписи возможно расширение видов электронных подписей, используемых для подписания цифрового согласия.

Права пользователя в инфраструктуре Цифрового профиля определяются после прохождения процедур авторизации.

Порядок создания и форма цифрового согласия устанавливается уполномоченным федеральным органом исполнительной власти.

В настоящее время совершенствуются механизмы электронной подписи, например, разрабатывается облачная квалифицированная электронная подпись (ОКЭП).

ОКЭП будет возможно получить в аккредитованном уполномоченном удостоверяющем центре, в том числе дистанционно с использованием ЕСИА и единой биометрической системы (ЕБС), что позволит получать услуги без личного присутствия, используя для предоставления цифрового согласия и подписания необходимых документов с использованием любого устройства (компьютера, планшета, мобильного телефона).

В настоящее время в рамках работ АНО «Цифровая экономика» создается Национальная система управления

данными (НСУД) [4], которая представляет собой совокупность нормативных, правовых, организационных, методических и информационно-технологических механизмов, обеспечивающих деятельность участников НСУД в сфере создания, преобразования и использования государственных данных.

В рамках НСУД планируется разработать единую онтологию и методологические подходы к хранению, использованию и передаче данных внутри государственной среды и провести масштабную работу в области аудита архитектуры данных в информационных системах ведомств.

Взаимодействие цифрового профиля с НСУД показано на рис. 2.3 и будет осуществляться следующим образом:

– НСУД осуществляет аудит информационных систем органов власти, результатом которого будут являться в том числе реестры информационных систем и сведений, которые в них хранятся;

– формируется реестр «нативных» идентификаторов для доступа к сведениям в ГИС с привязкой к внутреннему идентификатору ЕСИА;

– в случае изменения «нативных» идентификаторов в мастер-системе, НСУД предоставляет обновление связки внутренний идентификатор ЕСИА — «нативный» идентификатор ГИС;

– в случае необходимости запроса сведений, которые не хранятся в ЕСИА, инфраструктура Цифрового профиля получает у НСУД информацию о мастер-системе, в которой хранятся такие сведения.

Архитектура Цифрового профиля предполагает возможность создания различных сервисов, показанных на рис. 2.4, которые позволят повысить удобство и качество оказания услуг как гражданам, юридическим лицам и индивидуальным предпринимателям, так и государственным органам и организациям, предоставляя им удобные инструменты для работы, анализа и управления данными.

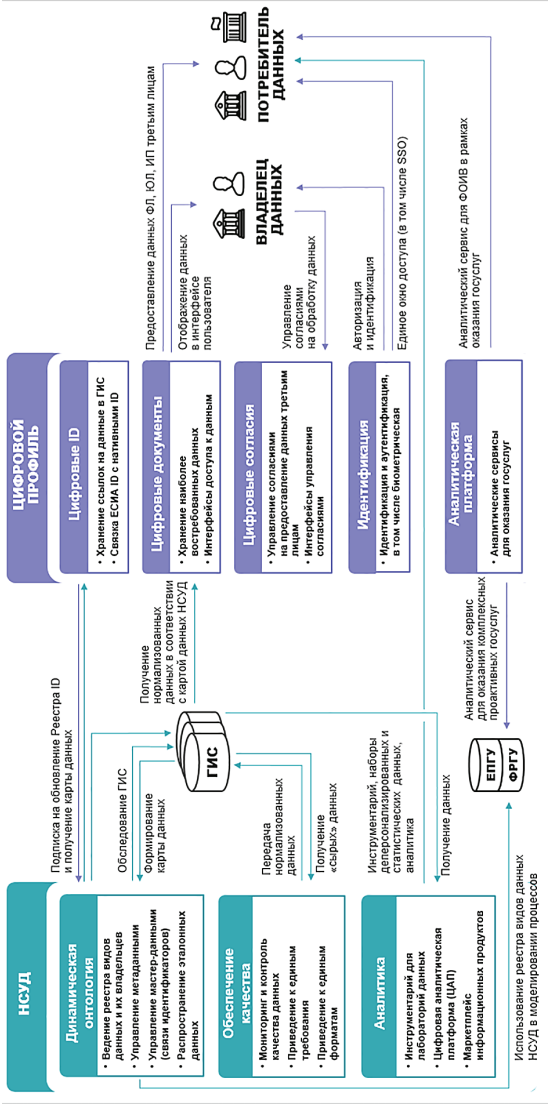


Рис. 2.3. Взаимодействие цифрового профиля и НСУД

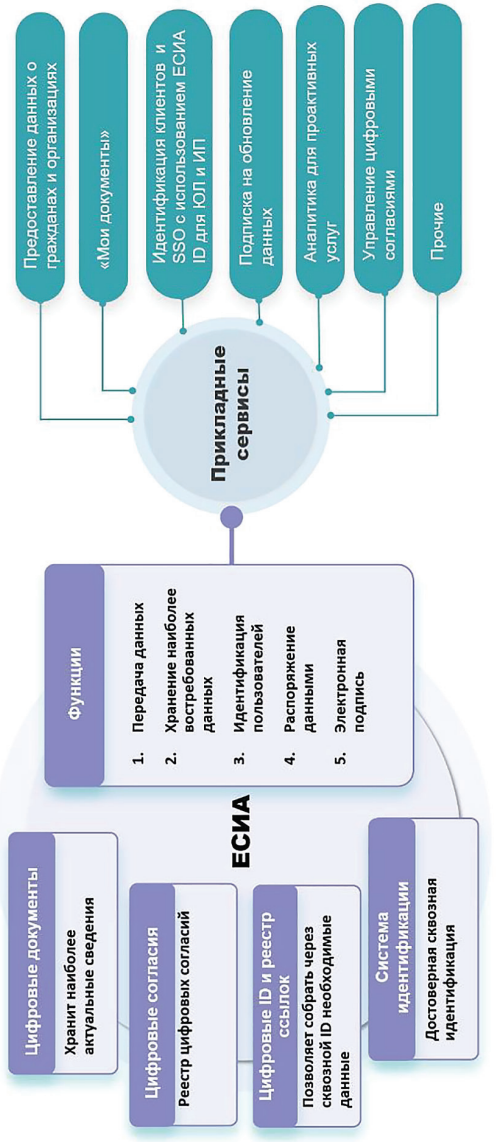


Рис. 2.4. Состав и структура сервисов

Основными функциями инфраструктуры Цифрового профиля являются:

– передача данных;
– хранение данных;
– идентификация пользователей;
– распоряжение данными;
– электронная подпись.

Инфраструктура Цифрового профиля (ИЦП) обеспечит для всех участников удобное информационное взаимодействие между пользователями данных (гражданин, государственные органы и организации, коммерческие организации, платформы и технологические стартапы) и ГИС путем передачи таких данных из различных источников через единый информационный канал.

ИЦП сохранит наиболее востребованные данные о человеке, в том числе необходимые для обеспечения идентификации и позволит идентифицировать каждого из участников процесса информационного взаимодействия в различных информационных системах.

Также ИЦП позволит реализовать передачу разрешений третьим лицам на хранение, обработку и получение данных гражданина, юридического лица и индивидуального предпринимателя, а также отзыв таких разрешений.

Инфраструктура Цифрового профиля позволит подтверждать волеизъявление участников процесса информационного взаимодействия через цифровые каналы и обеспечит возможность подписания документов и сведений в цифровом виде с использованием простой или квалифицированной электронной подписи.

Прикладными сервисами инфраструктуры Цифрового профиля являются:

– предоставление данных гражданам и организациям;
– «Мои документы»;
– идентификация клиентов и технология единого входа (Single Sign-on);
– подписка на обновление данных;
– аналитический сервис для проактивных услуг;

– управление цифровыми согласиями;
– прочие сервисы.

Получение государственных и коммерческих услуг требует заполнения большого количества документов. Цифровой профиль обеспечит государственным органам и коммерческим организациям удобный доступ к сведениям граждан и юридических лиц, содержащимся в Цифровом профиле (включая данные в ГИС, доступные по ссылкам), с их согласия и позволит организациям оказывать услуги более качественно, быстро, а также снизить издержки организаций на предоставление услуг.

Архитектура Цифрового профиля также будет содержать систему личных цифровых документов, в которой будет обеспечиваться хранение и актуализация наиболее востребованных юридически значимых сведений.

Такая система позволит хранить документы и сведения владельца данных, а также использовать цифровые документы для подтверждения личности через личный кабинет в мобильном приложении и на сайте.

ЕСИА может выступать поставщиком идентификации клиентов для различных коммерческих компаний при оказании услуг. Сервис единого входа позволит избежать необходимости повторного подтверждения личности и ее проверки, в том числе при личном присутствии. Поставщик идентификации (ЕСИА) проведет проверку и направит данные поставщику услуги.

Реализация такого сервиса позволит повысить защищенность граждан и организаций при оказании им услуг, а также упростит сам процесс получения услуги.

Данные граждан и юридических лиц могут изменяться, что обуславливает необходимость их обновления и актуализации.

Сервис обновления данных на базе инфраструктуры Цифрового профиля позволит государственным органам и коммерческим организациям получать актуальные данные путем подписки на обновления определенных сведений о гражданине и юридическом лице.

Аналитический сервис для проактивных услуг позволит государственным органам и организациям, оказывающим услуги, информировать граждан, юридических лиц и индивидуальных предпринимателей о необходимых им услугах на основании сведений в ГИС.

Все действия с цифровыми согласиями будут отражаться в едином реестре цифровых согласий и доступны в личном кабинете.

С использованием графического интерфейса инфраструктуры Цифрового профиля (личного кабинета) возможно просмотреть все выраженные гражданином согласия; предоставить или отозвать предоставленное цифровое согласие, в том числе внести изменения в ранее выданное согласие (только для действующего, ранее выраженного согласия);

На базе инфраструктуры Цифрового профиля могут быть созданы различные сервисы иными организациями, в том числе технологическими стартапами, что позволит улучшить пользовательский опыт, удовлетворенность получаемыми услугами, а также реализовать потребности участников обмена данными, возникающие в процессе информационного взаимодействия, посредством использования Цифрового профиля.

Механизм работы Цифрового профиля

Владелец данных — физическое лицо может воспользоваться сведениями из своего Цифрового профиля самостоятельно через интерфейс доступа (личный кабинет) Цифрового профиля, как показано на рис. 2.5.

При обращении за услугой данные из Цифрового профиля передаются организации после предоставления цифрового согласия (рис. 2.6).

Кроме интерактивного режима взаимодействия гражданина с инфраструктурой Цифрового профиля, получение данных из цифрового профиля гражданина возможно с использованием действующего механизма «черновиков».

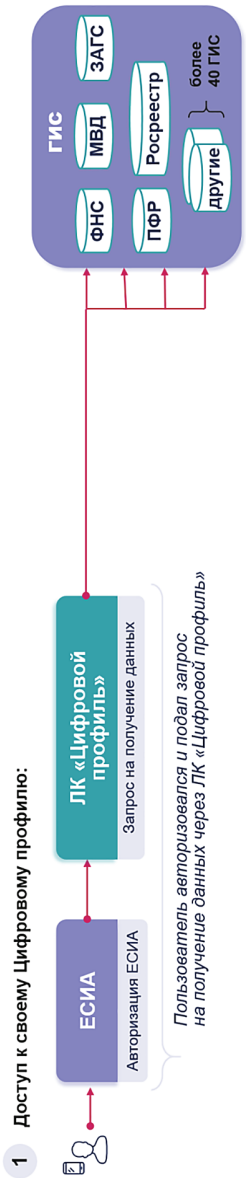


Рис. 2.5. Процесс работы физического лица с данными Цифрового профиля

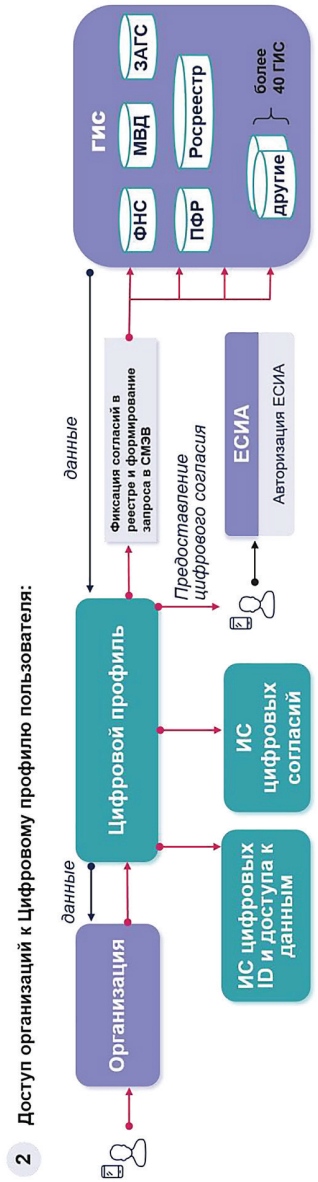


Рис. 2.6. Процесс работы организации с данными Цифрового профиля

Предоставление данных из Цифрового профиля может осуществляться только с согласия самого владельца профиля, за исключением случаев межведомственного взаимодействия, предусмотренных законодательством, когда государственные органы и организации могут получать персональные данные без его согласия в рамках оказания услуг, выполнения государственных функций или осуществления мероприятий, связанных с оперативно-розыскной деятельностью.

Для предоставления цифрового согласия владелец данных должен пройти идентификацию с использованием ЕСИА (в отдельных случаях, предусмотренных законодательством — Единой биометрической системы), а также подписать цифровое согласие простой или квалифицированной электронной подписью, а в отдельных установленных законодательно случаях после проведения биометрической идентификации с использованием единой биометрической системы. Использование простой электронной подписи регламентируется постановлением Правительства от 25 января 2013 года № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» [5]. Инфраструктура Цифрового профиля использует данные, хранящиеся в ГИС с его согласия, предоставленного в цифровом виде.

С помощью инфраструктуры Цифрового профиля будет возможно отправить запрос на корректировку данных непосредственно в источник данных (мастер-систему).

Процесс корректировки изображен на рисунке 2.7.

Процесс корректировки данных состоит из 4-х этапов:

1. Идентификация владельца данных с помощью ЕСИА (в отдельных случаях, предусмотренных законодательством — Единой биометрической системы).

2. Направление запроса в соответствующий ГИС на обновление данных в источнике через личный кабинет Цифрового профиля (в том числе в мобильном приложении).

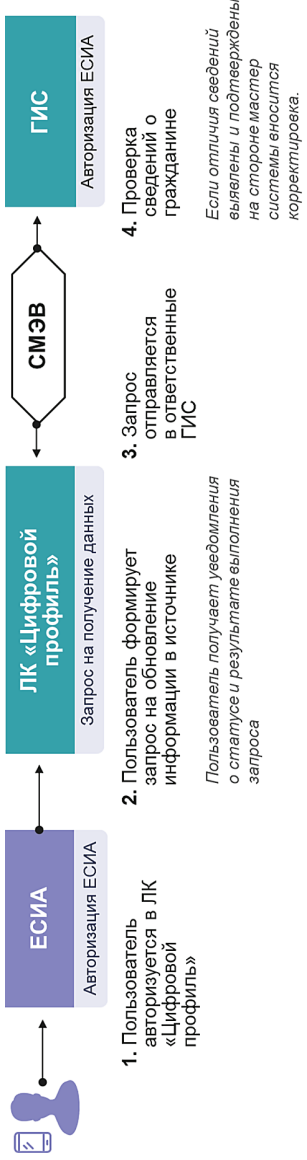


Рис. 2.7. Корректировка данных в цифровом профиле

3. Проверка сведений ответственным государственным органом, которому принадлежит ГИС, и корректировка данных в ГИС (при необходимости).

4. Направление ответа о корректировке/удалении или сохранении в неизменном виде запрашиваемых данных в личный кабинет Цифрового профиля.

В инфраструктуре Цифрового профиля будет обеспечена возможность блокировкии или ограничения доступа к данным о лицах, подлежащих государственной защите.

Высокие требования к конфиденциальности персональных данных предопределяют выбор организационно-правовой модели. Развитие и эксплуатация инфраструктуры Цифрового профиля будут осуществляться в рамках государственного контракта, заключенного между оператором инфраструктуры — Министерством цифрового развития, связи и массовых коммуникаций РоссийскойФедерации и технологическим исполнителем.

Такая модель не исключает возможности оказания услуг по организации доступа

к данным как на возмездной основе (для коммерческих пользователей), так и безвозмездной (для государства и, возможно, в иных случаях, установленных законом).

Возмездный доступ к услугам способствует развитию и модернизации государственных информационных систем, а также уменьшению нагрузки нецелевых запросов, составляющих в настоящее время значительную часть нагрузки на инфраструктуру электронного правительства.

Возмездный доступ к данным должен базироваться на следующих принципах:

- равные условия доступа участников к данным (недискриминационный доступ), в том числе в отношении оператора Цифрового профиля;
- использование дифференцированного тарифа в зависимости от создаваемой нагрузки;
- экономическая оправданность тарифа в сравнении с текущими расходами пользователей на получение аналогичных данных.

Размер и порядок взимания платы будет определен Правительством Российской Федерации.

В целевом состоянии инфраструктура Цифрового профиля масштабируется по объёму обрабатываемой информации, а также по производительности путём модернизации используемого комплекса технических средств без модификации программного обеспечения.

Инфраструктура Цифрового профиля проектируется и вводится в действие на перспективу с учётом расширения сферы её использования.

Согласно ГОСТ 27.003—90 «Состав и общие правила задания требований по надёжности» [6], инфраструктура Цифрового профиля относится к обслуживаемым изделиям общего назначения многократного циклического применения. Надёжность инфраструктуры Цифрового профиля определяется уровнем безотказности и способностью к восстановлению.

При проектировании инфраструктуры Цифрового профиля обеспечивается устойчивость по отношению к:

- программно-аппаратным ошибкам,
- отказам технических и программных средств с возможностью восстановления работоспособности и целостности информации.

Показатели надёжности инфраструктуры Цифрового профиля обеспечиваются и их количественные значения приведены на рис. 2.8.

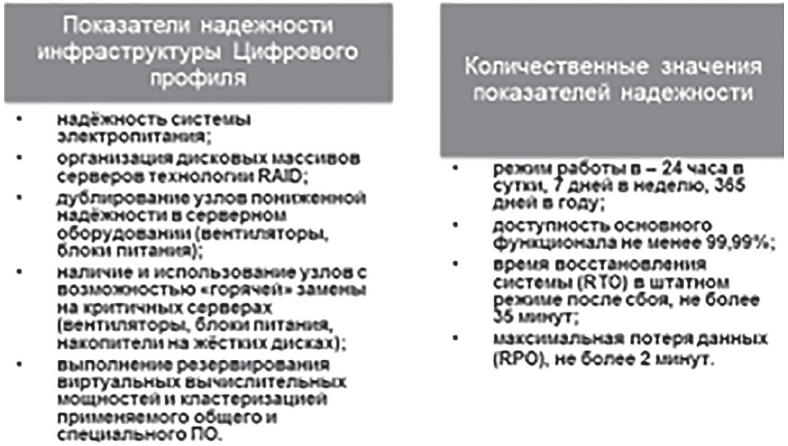


Рис. 2.8. Показатели надежности инфраструктуры Цифрового профиля

2.3. Обеспечение информационной безопасности цифрового профиля

При построении инфраструктуры цифрового профиля необходимо обеспечить конфиденциальность, целостность и доступность обрабатываемой информации, защиту процессов взаимодействия и обмена между источниками и потребителями данных.

Безопасность и устойчивость к компьютерным атакам инфраструктуры цифрового профиля обеспечивается

посредством создания условий безопасного и устойчивого функционирования вычислительной инфраструктуры всех взаимодействующих систем и применения безопасных технологий обработки информации.

Обеспечение безопасности и устойчивости в рамках проекта должно являться комплексным решением, которое предполагает гармонизацию и реализацию требований законодательства Российской Федерации, требований регулирующих и надзорных органов, отраслевых стандартов, универсального комплекса государственных стандартов, регламентирующих защиту информации и обеспечение непрерывности деятельности. Решение должно учитывать актуальные риски и угрозы, а также соответствовать лучшим мировым практикам.

Обеспечение информационной безопасности при осуществлении взаимодействия между сторонами, подтверждении цифрового согласия, неотказуемости от действий, целостности передаваемой информации осуществляется посредством применения инструментов электронной подписи в соответствии с требованиями уполномоченного органа в области обеспечения безопасности.

Для доступа к обрабатываемым сведениям применяются технологии строгой идентификации и аутентификации с использованием усиленных механизмов защиты.

Уровни обеспечения защищенности информационных систем-источников различных государственных ведомств и организаций отличаются. При организации взаимодействия между участниками следует сформировать доверенную среду с одинаково высоким уровнем информационной безопасности систем-участников.

В инфраструктуре Цифрового профиля определен следующий порядок доступа участников к видам сведений, хранящимся в Цифровомпрофиле:

– владельцы данных (граждане, юридические лица, индивидуальные предприниматели) будут иметь права доступа на чтение данных из инфраструктуры Цифрового

профиля, а также запись данных в части следующих сведений, относящихся к конкретному физическомулицу:

- мобильный телефон,
- домашний телефон,
- e-mail,
- домашний адрес;

– поставщики данных будут иметь права доступа на чтение данных в рамках запросов к инфраструктуре Цифрового профиля, а также права записи данных в части сведений, для которых их информационные системы будут являться «мастер-системами»;

– потребители данных будут иметь права на чтение данных в инфраструктуре Цифрового профиля в рамках соответствующих запросов.

У потребителей данных не будет прав на запись данных в инфраструктуру Цифрового профиля.

Для обеспечения информационной безопасности инфраструктуры Цифрового профиля:

– разрабатывается модель угроз безопасности обрабатываемой информации и действий нарушителя;

– проводится согласование разработанных моделей угроз безопасности информации и действий нарушителя, а также проекты по созданию основанных на них систем защиты информации с федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России);

– внедряется система защиты информации в соответствии с разработанной моделью угроз безопасности обрабатываемой информации и действий нарушителя.

При разработке систем защиты информации необходимо учесть следующие предпосылки:

– система защиты информации должна разрабатываться в рамках информационной системы в целом по отдельному специальному техническому заданию;

– система защиты информации должна обеспечить целостность и доступность информации, хранящейся и обрабатываемой в рамках соответствующей информационной системы, конфиденциальность информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, идентификацию и аутентификацию субъектов доступа (пользователей и процессов) к объектам доступа, установление авторства размещаемой в информационной системе информации;

– система защиты информации должна содержать в своем составе подсистему учета обращений к цифровым профилям и цифровым согласиям, а также учета обращений к информационным ресурсам информационных систем, взаимодействующих с ней (далее — подсистема биллинга), фиксирующих в том числе время, субъект, объект и результат каждого обращения (транзакции);

– подсистема биллинга систем защиты информации должна обеспечивать неотказуемость каждой транзакции;

– должны быть обеспечены целостность и некорректируемость журналов учета обращений подсистемы биллинга систем защиты информации;

– используемые в системе защиты информации средства защиты информации должны соответствовать требованиям, определяемым исходя из модели угроз безопасности обрабатываемой информации и действий нарушителя. Средства криптографической защиты информации должны иметь подтверждение соответствия таким требованиям, установленным ФСБ России. Некриптографические средства защиты информации должны иметь сертификаты соответствия таким требованиям, установленным ФСТЭК России;

– системой защиты информации должны реализовываться процессы обнаружения, предупреждения и ликвидации компьютерных атак во взаимодействии с Национальным координационным центром по компьютерным инцидентам.

Требования к обеспечению определенных классов защиты Цифрового профиля определяются на этапе проектирования Цифрового профиля в рамках формирования модели угроз.

Требования к уровню защищенности персональных данных и классу защиты систем в инфраструктуре Цифрового профиля могут быть пересмотрены на этапе проектирования Цифрового профиля с учетом дополнительных сведений, содержащихся в Цифровом профиле.

После модернизации систем инфраструктуры Цифрового профиля проводятся аттестационные испытания измененных модулей.

Защита персональных данных цифрового профиля осуществляется в соответствии с требованиями, определяемыми Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7] и Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [8]

Формируется модель угроз инфраструктуры Цифрового профиля с учетом модели угроз, существующих в Единой системе идентификации и аутентификации, и модели угроз, существующих в Единой биометрической системе, и разрабатывается план поэтапной модернизации ЕСИА в части перехода на отечественное программное обеспечение и российские средства защиты.

Средства криптографической защиты информации должны иметь подтверждение соответствия таким требованиям, установленным ФСБ России.

Для обеспечения защиты от несанкционируемого доступа используются средства защиты не ниже 4 класса защищенности по требованиям ФСТЭК. Для прикладного ПО проводится анализ как программного кода на отсутствие НДВ по 4 классу, так и анализ защищенности всей системы.

Системой защиты информации должны реализовываться процессы обнаружения, предупреждения и ликвидации компьютерных атак во взаимодействии с Национальным координационным центром по компьютерным инцидентам.

Кроме того, предусматривается отделение механизма информирования граждан и юридических лиц о существующем профиле цифровых согласий (без возможности внесения в них изменений) от механизма внесения изменений в цифровые согласия.

Внесение изменений в цифровые согласия (предоставление или отзыв) при запросе государственной (муниципальной, коммерческой) услуги планируется обеспечивать с использованием усиленной квалифицированной электронной подписи (КЭП) или облачной квалифицированной электронной подписи (ОКЭП) с указанием срока действия такого согласия.

Доступ к инфраструктуре Цифрового профиля с целью обновления цифрового профиля гражданина или организации предоставляется в соответствии с регламентом обновления данных из ГИС и ограничен только полномочиями государственными органами, государственными внебюджетными фондами, органами местного самоуправления с использованием СМЭВ.

Доступ иных организаций к инфраструктуре Цифрового профиля ограничивается только функцией использования цифрового профиля в соответствии с категорией организации и матрицы доступа к данным и предоставляется через СМЭВ или другие каналы предоставления данных с соответствующим уровнем безопасности.

Идентификация физического или юридического лица инфраструктуры Цифрового профиля осуществляется с использованием механизмов ЕСИА.

Для доступа к персональным данным пользователя и управления цифровыми согласиями в дополнение к механизмам аутентификации ЕСИА используется удаленная идентификация (биометрическая верификация).

Все запросы и заявки пользователей, сформированные в инфраструктуре Цифрового профиля при взаимодействии с другими ГИС подписываются с использованием КЭП или ОКЭП, полученным в аккредитованном удостоверяющем центре, для обеспечения их юридической значимости.

В целях защиты от угроз нарушения целостности, достоверности и конфиденциальности в инфраструктуре Цифрового профиля при обработке и хранении персональных данных физических лиц и данных юридических лиц, формировании соответствующих реестров согласий и ссылок на данные в ГИС используются средства криптографической защиты информации (далее — СКЗИ) класса не ниже КВ по требованиям ФСБ.

Планируется реализовать механизмы шифрования базы данных цифрового профиля, которые будут поддерживать возможность смены ключей при окончании их срока действия, кластеризации данных на разных ключах, возможность безопасного резервного копирования и восстановления данных при аварии.

В инфраструктуре цифрового профиля в процессе идентификации при формировании и обработке токенов авторизации с использованием ГОСТ, в целях защиты от угроз нарушения целостности и конфиденциальности используется СКЗИ класса не ниже КС3 по требованиям ФСБ.

Обеспечение защищенного взаимодействия между пользователем и инфраструктурой цифрового профиля осуществляется с использованием СКЗИ класса не ниже КС1 на стороне пользователя и СКЗИ класса не ниже КС3 на стороне инфраструктуры Цифрового профиля.

При формировании и передаче данных ГИС в инфраструктуре Цифрового профиля в целях защиты от угроз нарушения целостности и достоверности используется СКЗИ класса не ниже КВ.

При передаче данных между ГИС и инфраструктурой Цифрового профиля в целях защиты от угроз нарушения

целостности и конфиденциальности используется СКЗИ класса не ниже КС3.

При формировании и передаче данных инфраструктурой Цифрового профиля во внешние организации, в целях защиты от угроз нарушения целостности и достоверности планируется использовать СКЗИ класса не ниже КВ.

При формировании запросов и передаваемых данных от внешних организаций в инфраструктуру Цифрового профиля, в целях защиты от угроз нарушения целостности и достоверности используется СКЗИ класса не ниже КС3.

При передаче данных между инфраструктурой Цифрового профиля и внешними организациями в целях защиты от угроз нарушения целостности и конфиденциальности используется СКЗИ класса не ниже КС3.

Пилотный проект по реализации концепции цифрового профиля и ожидаемые эффекты от использования цифрового профиля

Дорожная карта создания Цифрового профиля состоит из трёх основны хэтапов:

1. Принятие ФЗ о Цифровом профиле [9] и подзаконных актов. Срок выполнения 31 марта 2020 года.

2. Проведение подготовительных мероприятий для запуска эксперимента. Срок выполнения 30 апреля 2019 года.

3. Осуществление пилотного проекта. Срок выполнения 31 марта 2020 года.

Введение Цифрового профиля в промышленную эксплуатацию планируется к концу сентября 2020 года.

Реализация целевого функционала инфраструктуры Цифрового профиля прежде всего зависит от сроков принятия нормативно-правовых актов, реализации мероприятий по созданию НСУД и доработке информационных систем органов власти, которые являются мастер-системами по предоставлению данных о гражданах и юридических лицах.

В связи с этим планируется поэтапная реализация целевой архитектуры Цифрового профиля, первый этап которой запланирован на конец 2019 года (пилотная реализация).

В рамках первого этапа планируется реализация инфраструктуры Цифрового профиля для передачи данных о физических лицах, которые хранятся в мастер-системах в электронном виде и могут предоставляться через указанную инфраструктуру в режиме реального времени. Расширение перечня данных о гражданах и реализация функциональности для юридических лиц предусмотрены на следующих этапах.

Реализация целевой архитектуры Цифрового профиля во многом зависит от модернизации ГИС и их готовности предоставлять сведения в режиме реального времени. В частности, получение и обновление данных в рамках целевой реализации архитектуры Цифрового профиля невозможно без такой доработки, что накладывает ограничения на объем пилотного проекта. В этой связи принято решение о совместной пилотной реализации (эксперимент) инфраструктуры Цифрового профиля и НСУД.

В рамках проверки гипотезы в отношении инфраструктуры Цифрового профиля будут решаться следующие задачи:

– возможности предоставления данных из государственных информационных систем;

– сокращения времени предоставления данных;

– предоставления данных в одном пакете и удобном формате;

– реализации права гражданина распоряжаться своими данными (функционирование инфраструктуры управления цифровыми согласиями);

– эффективности реализации ссылочной модели для доступа к данным.

В рамках пилотного проекта Цифрового профиля планируется реализация трех сервисов инфраструктуры

Цифрового профиля, интегрированных с информационными системами органов власти и коммерческими информационными системами банков-участников пилотного проекта:

1. Сервис по предоставлению данных физического лица (данных из Цифрового профиля и ГИС, по ссылочной модели) с его согласия банку-участнику пилотного проекта для заполнения анкеты на получение кредитного продукта.

2. Сервис уведомлений банков-участников об изменениях в видах сведений граждан (для подписавшихся банков).

3. Сервис по предоставлению гражданину в мобильном приложении графического интерфейса взаимодействия с двумя модулями Цифрового профиля, а именно «Мои документы» и «Цифровые согласия».

В таблице 2.1 представлена основная функциональность подсистем инфраструктуры Цифрового профиля на конец 2019 года в сравнении с функциональностью целевой архитектуры.

Таблица 2.1

Пилотная реализация (конец 2019 года)	**Целевая реализация**
Общая функциональность	
Юридическая значимость получаемых сведений зависит от изменения законодательства и плана мероприятий НСУД	Юридическая значимость записей в мастер-системах
Функционал Цифрового профиля реализован для физических лиц в ограниченно мобъеме	Функционал Цифрового профиля реализован для физических и юридических лиц
Цифровые документы	
Хранение ограниченного перечня, которые доступны для получения из ИС органов власти	Хранение полного состава данных

Продолжение табл. 2.1

Пилотная реализация (конец 2019 года)	**Целевая реализация**
Актуализация сведений Цифрового профиля данными из информационныхсистем органов власти, которые будут интегрированы (при наличии технической возможности) с инфраструктурой Цифрового профиля в рамках пилотного проекта	Актуализация сведений Цифрового профиля данными из информационных систем органов власти, которые будут интегрированы с инфраструктурой Цифрового профиля в целевой схеме
Offline-доступ к видам сведений через мобильное приложение	Offline-доступ к видам сведений через мобильное приложение
Система идентификации	
Реализация возможностииденти фикации граждан с помощью ЕСИА и при необходимости ЕБС при предоставлении коммерческих услуг	Реализация возможности идентификации граждан с помощью ЕСИА и при необходимости ЕБС при предоставлении коммерческих услуг
Технология единого входа	Технология единого входа
Цифровые согласия	
Юридическая значимость цифровых согласий (с помощью ПЭП ЕСИА, в некоторых случаях ПЭП ЕСИА после проведения удаленной идентификации с использованием ЕБС)	Юридическая значимость цифровых согласий (в том числе с помощью УКЭП или ОКЭП)
Управление цифровыми согласиями	Управление цифровыми согласиями
Предоставление доступа к видам сведений для третьих лиц с согласия владельца сведений	Предоставление доступа к видам сведений для третьих лиц с согласия владельца сведений

Окончание табл. 2.1

Пилотная реализация (конец 2019 года)	**Целевая реализация**
Цифровые ID и реестр ссылок	
Хранение реестра ссылок на источники данных и обновление данных реестра данными из информационных систем органов власти, которые будут интегрированы (при наличии технической возможности) с инфраструктурой Цифрового профиля в рамках пилотного проекта	Хранение реестра ссылок на источники данных
Хранение реестра цифровых идентификаторов и обновление данных реестра данными из информационных систем органов власти, которые будут интегрированы (при наличии технической возможности) с инфраструктурой Цифрового профиля в рамках пилотного проекта	Хранение и обновление реестра цифровых идентификаторов с помощью НСУД
Информационная безопасность	
Использование СМЭВ (для органов власти) или иного канала класса КС3	Использование СМЭВ или иного канала класса КС3
Целостность и конфиденциальность информации обеспечена с использованием криптографического оборудования	Целостность и конфиденциальность информации обеспечена с использованием криптографического оборудования
OpenID Connect со встроенной отечественной криптографией по классу КС3 для передачи персональных данных	OpenID Connect со встроенной отечественной криптографией по классу КС3 для передачи персональных данных

Участники реализации концепции Цифрового профиля и их роли представлены в таблице 2.2.

Таблица 2.2

Ведомство	Роль
Минкомсвязь России	– Оператор платформы Цифровой профиль; – Центр компетенции (разработка концепции, изменений в НПА, построение системы)
Банк России	Центр компетенции (разработка концепции, изменений в НПА, построение системы)
ПАО «Ростелеком»	Соисполнитель в рамках федерального проекта «Информационная инфраструктура» [10] национальной программы «Цифровая экономика Российской Федерации»
Государственные органы	Операторы ГИС
АНО «Цифровая экономика»	Центр компетенции мероприятий программы «Цифровая экономика»
Аналитический центр при Правительстве Российской Федерации	Центр компетенции по реализации НСУД
Ассоциация Финтех	Организатор взаимодействия с банковским сообществом в процессе реализации пилотного проекта
Федеральные органы исполнительной власти, уполномоченные в области осуществления контроля в области персональных данных и защиты информации	Осуществление государственного контроля за обработкой и защитой персональных данных

В итоге, создание инфраструктуры Цифрового профиля будет способствовать повышению доступности коммерческих, государственных и иных услуг в электронном виде, осведомленности об этом граждан и организаций, и их удовлетворенности.

Для граждан и юридических лиц использование инфраструктуры Цифрового профиля позволит обеспечить:

– получение цифровых услуг;

– уменьшение стоимости услуг за счет перевода их в цифровую форму;

– сокращение времени и количества шагов для получения услуг в цифровом виде;

– управление своими данными в режиме 365/7/24.

Дляорганизаций использование инфраструктуры Цифрового профиля позволит обеспечить:

– предоставление услуг организациям полностью в цифровом виде;

– повышение операционной эффективности за счет увеличения объема данных, используемых в принятии управленческих решений;

– повышение качества, доступности и скорости предоставления данных;

– сокращение времени и количества шагов для открытия и ведения бизнеса («в один клик»);

– появление новых сервисов и бизнес-моделей, основанных на обработке и анализе данных;

– обеспечение возможности получения согласия на передачу и обработку персональных данных в цифровом виде.

Создание Цифрового профиля будет содействовать развитию цифровой экономики и позволит:

– повысить эффективность управленческих решений за счет увеличения объема данных, обрабатываемых в автоматизированном виде;

– обеспечить перевод ГИС на реестровую модель формирования, ведения и предоставления данных;

– обеспечить возможность использования государственными органами и организациями данных полностью в цифровом виде в целях предоставления государственных услуг;

– обеспечить возможность использования государственными органами цифровых технологий для снижения регуляторной нагрузки на организации;

– обеспечить возможность исключения дублирования данных (дедупликация) в разных информационных ресурсах, кроме дублирования наиболее востребованных видов сведений в ЕСИА с целью снижения нагрузки на каналы передачи данных;

– повысить безопасность при обмене данными;

– обеспечить развитие ГИС и снижение на них нагрузки.

Для количественной и качественной оценки реализации Цифрового профиля предусматриваются показатели эффективности, приведенные в таблице 2.3.

Ключевые показатели эффективности для коммерческих организаций представлены в таблице 2.4.

Использование Цифрового профиля позволит банкам в автоматическом режиме запрашивать у ГИС соответствующие данные по доходам клиента, проверять достоверность документов, удостоверяющих личность, загружать в автоматическом режиме во внутренние учетные системы банка полученную информацию, что позволит существенно сократить время формирования необходимого пакета документов и время принятия решения по предоставлению клиентам финансовых услуг. Таким образом, банк может существенно снизить операционные издержки за счет получения актуальных и проверенных данных в удобном формате.

Количественная оценка (снижение временных и денежных издержек) ключевых показателей эффективности для коммерческих организаций будет проработана после проведения пилотного проекта.

Таблица 2.3

Показатель	Время	Качественная характеристика
Доступность государственных и коммерческих услуг в результате их перевода в электронный вид	Сейчас: 247/5/8 Станет: 365/7/24	Перевод до 80% всех услуг в электронный вид
Сокращение количества шагов для заполнения анкет и заявлений	Было: ~ 30 минут Станет: несколько секунд	Оказание услуг в 3 клика
Сокращение количества бумажных документов, необходимых для получения услуг	Сокращение времени на поиск бумажных документов, копирование (при необходимости) и нотариальное заверение документов (при необходимости)	По базовым сведениям, в ЕСИА — безбумажный По остальным — сокращение до 80%
Сокращение количества личных посещений	Сокращение времени на личное посещение	До 1 личной явки
Распоряжение личными данными	Сейчас: 247/5/8 Станет: 365/7/24	Интерактивное распоряжение

Таблица 2.4

Показатель	Качественная характеристика
Сокращение операционных издержек на идентификацию, подтверждение и обновление данных	Предоставление достоверных государственных данных онлайн
Сокращение количества личных посещений	До 1 явки
Сокращение процента ошибок при заполнении анкет пользователями	Снижение процента ошибок (будет рассчитано позднее)

Окончание табл. 2.4

Показатель	Качественная характеристика
Сокращение количества бумажных документов, требуемых для оказания услуги	Сокращение бумажного оборота до 80%
Сокращение количества шагов, требуемых для оказания услуги	3 клика

Показателями эффективности реализации цифрового профиля для государственных органов могут выступать показатели, приведенные в таблице 2.5.

Таблица 2.5

Показатель	Качественная характеристика
Увеличение количества услуг, предоставляемых в электронном виде	До 80% всех услуг
Увеличение количества услуг, оказываемых проактивно и комплексно	До 80% от переведенных в электронный вид
Сокращение количества шагов по заполнению заявлений на предоставление госуслуг	3 клика
Сокращение количества межведомственных запросов	Снижение на 75%
Сроки исполнения государственных услуг	Срок получения услуги сократится на 70%
Сокращение количества бумажных документов, необходимых для оказания услуг	Сокращение бумажного оборота до 80%

Вопросы для самоконтроля

1. Определите понятие «Цифровой профиль гражданина».
2. Определите понятие «Цифровой профиль организации».
3. Проанализируйте последствия и преимущества введения цифровых профилей.

4. Как обеспечивается механизм работы Цифрового профиля?
5. Что включает архитектура Цифрового профиля?
6. Охарактеризуйте три сервиса инфраструктуры Цифрового профиля, реализация которых планируется в рамках пилотного проекта.

Список использованных источников главы 2

1. Программа «Цифровая экономика Российской Федерации»: [Электронныйресурс] // Правительство РФ. — М., 2018. — URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf/ (Датаобращения: 28.10.2019).
2. Указ Президента России от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»: [Электронныйресурс] — URL: http://www.kremlin.ru/acts/bank/43027 (Дата обращения: 28.10.2019).
3. Федеральный закон от 25.04.2002 № 40-ФЗ (ред. от 01.05.2019) «Об обязательном страховании гражданской ответственности владельцев транспортных средств»: [Электронный ресурс] — URL: http://www.consultant.ru/document/cons_doc_LAW_36528/ (Дата обращения: 28.10.2019).
4. Концепция и дорожная карта НСУД: [Электронный ресурс] — URL: https://digital-api.ac.gov.ru/upload/iblock/53c/Концепция и дорожная карта НСУД.PDF (Дата обращения: 28.10.2019).
5. Постановление Правительства РФ от 25.01.2013 № 33 (ред. от 20.11.2018) «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»: [Электронный ресурс] — URL: http://www.consultant.ru/document/cons_doc_LAW_141712/ (Дата обращения: 28.10.2019).

6. ГОСТ 27.003—90. Надежность в технике. Состав и общие правила задания требований по надежности: [Электронный ресурс] — URL: http://docs.cntd.ru/document/gost-27—003—90/ (Дата обращения: 28.10.2019).

7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 18 марта 2019 года) (редакция, действующая с 1 октября 2019 года): [Электронный ресурс] — URL: http://docs.cntd.ru/document/901990051 (Дата обращения: 28.10.2019).

8. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: [Электронный ресурс] — URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (Дата обращения: 28.10.2019).

9. Проект федерального закона о цифровом профиле № 89871: [Электронный ресурс] — URL: https://regulation.gov.ru/projects#npa=89871 (Дата обращения: 28.10.2019).

10. Федеральный проект «Информационная инфраструктура» [Электронный ресурс] — URL: https://digital.ac.gov.ru/about/28#description (Дата обращения: 28.10.2019).

Глава 3
ЦИФРОВЫЕ ТЕХНОЛОГИИ

3.1. История развития цифровых технологий

Американские инженеры начали разработку цифровых технологий в середине XX века. Их методы были основаны на математических концепциях, предложенных немецким математиком XVII века Готфридом Вильгельмом Лейбницем, который предложил двоичную вычислительную систему. Его инновации вдохновили такие цифровые коды, как Американский стандартный код для обмена информацией (ASCII), который описывал объекты с помощью цифр.

Цифровые технологии — это базовый процесс. Оцифрованная информация записывается в двоичном коде комбинаций цифр 0 и 1, также называемых битами, которые представляют слова и изображения. Цифровая технология позволяет сжимать огромное количество информации на небольших по размеру устройствах хранения, которые можно легко сохранять и транспортировать. Оцифровка также ускоряет скорость передачи данных. Цифровые технологии изменили многие сферы деятельности человека, способы общения между людьми, формы получения образования. [7]

Телекоммуникации передачи сообщений строятся на цифровых методах. В начале 1980-х годов усовершенствованная волоконная оптика дала толчок к развитию цифровых сетей связи. Цифровая технология заменила аналоговые сигналы для многих видов телекоммуникаций,

например, для сотовых телефонов и кабельных систем. Аналого-цифровые преобразователи использовали импульсную кодовую модуляцию (ИКМ) для преобразования аналоговых данных в цифровые сигналы. По сравнению с аналоговыми передачами оцифрованные сигналы были менее искажены и могли легко дублироваться.

В 1998 году премьера коммерческого цифрового телевизионного вещания состоялась в США. Спутники связи, известные как спутники прямого вещания (DBS), передавали сжатые цифровые сигналы зрителям, по нескольким сотням телевизионных программ. Другие формы цифровой информации, включая аудиопрограммы, были переданы абонентам через спутник. На основании приказа федеральной комиссии по связи все широковещательные российские каналы начали переводиться на цифровые с января 2019 года. [3]

Цифровая печать с использованием технологий электрофотографии и форматирования данных изменила способ издания книг и журналов, сдачи документов в налоговую инспекцию и пенсионный фонд, а также оформление документов купли-продажи между организациями и т. д.

Электронный числовой интегратор и вычислитель (ENIAC) долгое время считался первым электронным цифровым компьютером.

В 1973 году суд вынес решение о нарушении патентных прав и объявил Джона В. Атанасова и Клиффорда Э. Берри из университета штата Айова изобретателями цифрового компьютера Atanasoff-Berry, и что ENIAC был основан на их дизайне (рис. 3.1).

В начале 2000-х цифровые компьютеры, начиная с ноутбуков и заканчивая интернет-сетями, были разных размеров и предназначались для различных типов задач.

Суперкомпьютеры выполняли сложные математические вычисления, анализировали огромные объемы данных, которые можно было хранить в виде цифровой информации на пластиковых дисках, используя метод точечной записи: «1 и 0» с применением лазера.

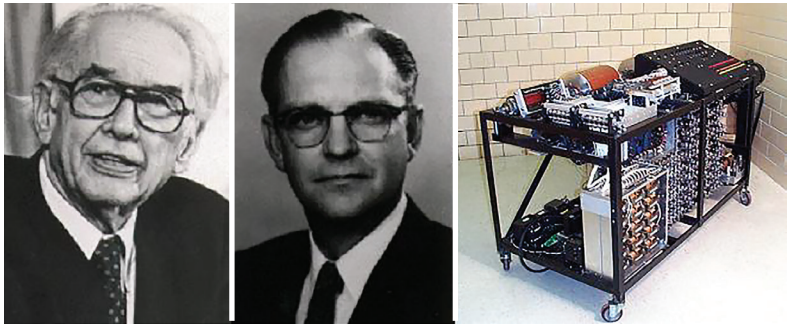


Рис. 3.1. Д. В. Атанасов, К. Э. Берри и первый в мире электронный цифровой компьютер Atanasoff-Berry (состоял из более 300 электровакуумных ламп)

К началу 2000-х годов цифровые камеры трансформировали фотографию, записывая цвета и интенсивность света с помощью пикселей. Кроме того, цифровое сжатие изображений и видео было достигнуто за счет кодов, разработанных комитетом экспертов со всего мира «Объединённая группа экспертов по фотографии» (Joint Photographic Experts Group, JPEG), и экспертной группой по движущимся изображениям (Moving Picture Experts Group, MPEG), основанных в рамках совместной работы Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC) — двух международных организаций по стандартизации, штаб-квартира которых расположена в Женеве (Швейцария). [9]

Анимация часто оцифровывалась, когда некоторые фильмы и мультфильмы создавались исключительно с помощью компьютеров.

Цифровая система передачи данных (DDBS) управляет воздушным движением. Цифровая рентгенография преобразует аналоговые сигналы рентгеновских лучей для создания цифровых изображений.

Цифровые технологии изменили почти все аспекты современной жизни. Путешествия, работа, покупки, раз-

влечения и связь — это лишь некоторые из областей, которые были революционизированы в последние десятилетия. Сейчас редко можно найти электронное устройство или механизм, который каким-либо образом не использует цифровые технологии.

Цифровые технологии означают, что устройства могут быть более компактными, быстрыми, легкими и более универсальными. Огромное количество информации может храниться локально или удаленно и перемещаться практически мгновенно. Даже термин «информация» расширился и включает в себя медиа: фотографии, аудио и видео, и больше не относится только к словам и цифрам.

3.2. Сферы применения цифровых технологий

Сферы, где применение цифровых технологий улучшило работу:

– социальная сеть;
– скорость передачи данных;
– «универсальная работа»;
– возможности обучения;
– автоматизация;
– хранение информации;
– редактирование;
– точное дублирование;
– GPS и картография;
– транспорт;
– низкая стоимость;
– развлечения;
– новости;
– военное дело;
– банковское дело и финансы;
– минимизация размера. [10]

Рассмотрим более подробно улучшение работы в каждой сфере.

1. Социальная сеть

Цифровые технологии позволяют легко оставаться на связи с друзьями, семьей и работать удаленно, даже

если вы находитесь в другой части мира. Вы можете общаться с помощью слов, видео, аудио и обмениваться другими средствами массовой информации. Веб-сайты, приложения и программное обеспечение были созданы, чтобы помочь пользователям в общении. С социальными сетями, обменом сообщениями, текстовыми сообщениями, ноутбуками, планшетами и мобильными телефонами никто не должен чувствовать себя изолированным в цифровом мире.

2. Скорость передачи данных

Скорость интернета увеличивается в геометрической прогрессии с первых дней коммутируемого доступа. Все более быстрая широкополосная связь позволяет практически мгновенно передавать большие объемы информации, передавать потоковое видео и аудио в режиме реального времени, отправлять большие файлы данных и получать доступ к данным через Интернет практически из любой точки мира.

3. «Универсальная работа»

Характер работы был преобразован с помощью цифровых технологий. Расширение возможностей подключения означает, что многие люди теперь имеют гораздо больше возможностей для работы из дома, поскольку удаленная работа становится все более распространенным явлением. Многие виды работы теперь можно выполнить за сотни или даже тысячи километров без каких-либо трудностей, без необходимости присутствия всех работников в одном здании. Теперь возможны многие другие гибкие методы работы.

4. Возможности обучения

Любой, кто имеет доступ к Интернету, имеет доступ к огромной доле мировых знаний через Интернет. Уроки и курсы можно изучать в режиме онлайн. Коммуникационный прогресс означает, что теперь можно легко общаться с большей частью населения мира и учиться непосредственно из источников — например, если изучать иностранный язык. Цифровые технологии также могут использоваться людьми с ограниченными возмож-

ностями, как в обучении, так и в трудоустройстве, что даем им равные возможности на рынке труда.

5. Автоматизация

Цифровые технологии делают машины умнее. В некоторых случаях машинам больше не нужны люди, чтобы ими управлять, освобождая рабочих от часто скучных задач для более интересных занятий. Продукты и услуги дешевеют по мере развития технологий и становятся все более распространенными. Многие задачи теперь могут выполняться непосредственно клиентами, а не через посредника — например, при бронировании билета.

6. Хранение информации

Цифровые технологии позволяют хранить большие объемы информации на носителях с небольшим объемом памяти.

Большие объемы мультимедиа, такие как фотографии, музыка, видео, контактная информация и другие документы, можно переносить на устройствах внешне малых размеров — таких как мобильные телефоны. С физической точки зрения местоположение данных может находиться в Интернете, что позволяет получить к ним доступ с любого устройства, имеющего выход в глобальную сеть.

Творческие возможности для редактирования видео и фотографий увеличились в геометрической прогрессии с появлением цифровых технологий. Технология является более доступной и простой в использовании, а то, что раньше требовало студии с дорогим оборудованием, теперь можно делать дома.

7. Редактирование

Одно из больших преимуществ цифровых технологий по сравнению с традиционными технологиями заключается в том, что информацию легче редактировать или обрабатывать. Обработка текста привела к революции в редактировании документов. Редактирование видео, которое раньше требовало дорогих студий и оборудования, теперь можно выполнять на ноутбуке в любом месте земного шара. Теперь доступны все виды фотографических эффектов, а также возможность творчески изменять изображения.

8. Точное дублирование

Одна из замечательных особенностей цифровых технологий заключается в том, что они обеспечивают точное дублирование информации. Например, вы можете написать рабочий отчет и отправить его по электронной почте нескольким получателям, или вы можете разослать несколько копий фотографий семье и друзьям. В области 3D-печати сейчас происходят прорывы в технологиях, которые, похоже, радикально преобразят наш мир.

9. GPS и картография

Раньше, пытаясь найти дорогу, люди обычно обращались к бумажной карте, но цифровые в сочетании со спутниковой технологии преобразили путешествия. Сервисы GPS теперь могут точно определять местоположение человека, сообщать ему о пробках и перекрытиях дорог в режиме реального времени, а также предоставлять много актуальной информации — такой как время прибытия в пункт назначения, а также альтернативные маршруты. Если необходимо найти открытую заправочную станцию, аптеку и т. д., то с помощью цифровых технологий, сервисов GPS это сделать легко.

10. Транспорт

Многие поезда и самолеты уже в определенной степени полагаются на цифровые технологии. Дорожные транспортные средства, такие как легковые и грузовые автомобили, станут полностью автоматизированными в недалеком будущем. Доступ к расписанию, а также бронирование билетов и мест в самолетах и поездах теперь часто происходит онлайн. В паспорта планируется внести цифровые чипы, которые будут хранить информацию, что позволит ускорить процесс регистрации и прохождения таможни и т. д.

11. Низкая стоимость

Отправка электронной почты, общение через видео с семьей и бронирование в Интернете, как правило, ничего

не стоят. Это предоставляет возможности для недорогого самообразования, создания бизнеса, покупки и продажи предметов или зарабатывания денег в Интернете.

12. Развлечения

Вся индустрия развлечений радикально изменилась. Многие люди получают удовольствие от общения в социальных сетях или от компьютерных игр. Традиционные средства массовой информации также эволюционировали: телевидение и радиовещание стали цифровыми.

13. Новости

Все больше людей получают новости в Интернете, или через веб-сайт, или через социальные сети. Даже традиционные средства массовой информации, такие как телевидение и радио, были оцифрованы. Люди имеют больше источников новостей, чем когда-либо, и большинство из них доступны 24 часа в сутки. Независимая и самостоятельная журналистика сейчас очень распространена, а также обычные люди, снимающие фото и видео на свои телефоны, могут выложить информацию в свободный доступ.

14. Военное дело

В Вооруженных силах применяют «русские рипперы» — ударные беспилотники большой дальности и «разведчики» — БПЛА, способные находить противника по радиоэлектронному излучению и с помощью радара. Аспекты работы аппаратов в боевых условиях: тактические приемы ведения разведки с помощью различных бортовых средств, порядок взаимодействия с заинтересованными родами войск, особенности технической эксплуатации комплексов в различных климатических условиях. Полученные данные обобщаются, всесторонне анализируются и вырабатываются рекомендации по применению комплексов в различных условиях обстановки.

15. Банковское дело и финансы

Нет сомнений, что цифровизация привела к революции в финансовых вопросах. Онлайн-банкинг, осуществляемый с помощью ноутбука, планшета или телефона, теперь стал нормой. Теперь пользователи банка

могут удаленно проверять свои входящие и исходящие платежи, а также организовывать денежные переводы и оплату счетов. Помимо банковской деятельности, другие финансовые вопросы, такие как покупка и продажа валюты и акций, могут решаться в режиме онлайн.

16. Минимизация размера

С развитием технологий размеры техники все уменьшаются: вспомните громоздкие компьютеры-ЭВМ, полвека назад занимающие целые залы, и сравните с ними современные ноутбуки весом менее 3 кг. И с каждым годом стремление к минимизации повседневной техники не ослабевает, человек пользуется уже не магнитолами, а цифровыми плеерами размером с брелок, не дисками для записи информации, а маленькими флеш-картами, устанавливает не камеры наблюдения, а незаметные видеорегистраторы.

Телефоны, которые мы носим с собой, — это, например, мини-компьютеры, которые позволяют осуществлять поиск информации в сети, работать в качестве калькуляторов, планировать поездки, снимать и воспроизводить фотографии, аудио и видео, игры, а также работать как телефоны и др.

Технологии будущего

Разработанные бизнесменами и учеными предварительные версии документов впервые были представлены на конференции «Цифровая индустрия промышленной России» (ЦИПР-2019) в Иннополисе.

В нацпроекте «Цифровая экономика» выделяются девять «сквозных» цифровых технологий: «большие данные» (bigdata), нейротехнологии и искусственный интеллект, системы распределенного реестра (блокчейн), квантовые технологии, новые производственные технологии, промышленный интернет, компоненты робототехники и сенсорика, технологии беспроводной связи (в частности, 5G), технологии виртуальной и дополненной реальности (VR и AR). Эти технологии считаются наиболее

перспективными, их применение ведет к радикальным изменениям существующих рынков, а также к появлению новых. По каждой из технологий будет подготовлена отдельная дорожная карта. [12]

Согласно нацпроекту «Цифровая экономика», эти документы должны учитывать потребности ведущих компаний в области цифровой экономики.

Каждая из крупных компаний, независимо от того, для чего она предназначена, инвестирует в технологии будущего.

Технологические тенденции, которые меняют мир, приближают человека к новому искусственному измерению и благосостоянию.

Технологические тенденции, которые развивают мир:

– Искусственный интеллект

Эта технология начала развиваться более 70 лет назад и основана на создании роботизированных систем, которые могут принимать решения так же, как и люди.

Термин «искусственный интеллект» был придуман американским ученым-компьютерщиком Джоном Маккарти в 1956 году и озвучен во время Дартмутской конференции. Сегодня это общий термин, который охватывает всё — от автоматизации роботизированных процессов до современной робототехники. В последнее время он приобрел известность, в частности, благодаря большим объемам данных, увеличению скорости, размера и разнообразия данных, с которыми работают компании. Искусственный интеллект может более эффективно, чем люди, выполнять такие задачи, как определение закономерностей в данных. [5]

Первые ученые, которые работали над созданием технологии, о которой говорилось во многих фантастических романах, изучали функционирование человеческого мозга. Цель этого исследования состояла в том, чтобы

иметь необходимые знания для создания компьютеров, которые работали бы подобно нейронным сетям мозга.

Спустя более семи десятилетий компьютеры все еще не полностью копируют функции человеческого мозга.

Аренд Хинце, доцент кафедры интегративной биологии и инженерии и компьютерных наук в Университете штата Мичиган, определил четыре типа искусственного интеллекта:

1. Реактивные машины. В качестве примера можно привести DeepBlue, шахматную программу IBM, которая победила Гарри Каспарова в 1990-х годах. DeepBlue может распознавать фигуры на шахматной доске и делать прогнозы, но он не имеет памяти и не может использовать прошлый опыт.

2. Ограниченная память. Эти системы искусственного интеллекта могут использовать прошлый опыт для формирования будущих решений. Некоторые из функций принятия решений в автономных транспортных средствах были разработаны таким образом. Наблюдения используются для информирования о действиях, которые произойдут в не столь отдаленном будущем. Эти наблюдения не хранятся постоянно.

3. Теория ума. Это психологический термин, относится к пониманию того, что у других есть свои убеждения, желания и намерения, которые влияют на принимаемые ими решения. Этот тип искусственного интеллекта еще не существует.

4. Самопознание. Возникновение искусственного сознания предполагает создание системы записи и почти вечного хранения информации на квантовом уровне — то есть на пространственно-временном промежутке без каких-либо вещественных носителей информационных массивов. Это означает, что человеку надо научиться записывать информацию в топологической структуре самого пространства или в глобальной виртуальной среде.

Самосознательные машины понимают свое текущее состояние и могут использовать информацию, чтобы

определить, что чувствуют другие. Этот тип искусственного интеллекта еще не существует. [9]

– Виртуальная реальность

Первоначально было трудно представить, что устройство виртуальной реальности имеет функцию, отличную от развлекательной. Сегодня виртуальная реальность вышла за рамки разработки развлекательных устройств:

– это может помочь общению людей, которые разделены расстоянием;

– это можно использовать при продаже товаров, предлагая клиентам более глубокое представление о товаре, который они хотят приобрести, посредством технологий виртуальной реальности;

– может быть использована для преодоления фобий и других тревожных расстройств (рис. 3.2).

Рис. 3.2. Применение виртуальной реальности при преодолении тревожных расстройств

– Blockchain

Это построенная на основе определенного алгоритма цепочка блоков финансовых транзакций. По своей сути блокчейн представляет собой инструмент для хранения

и передачи данных, который можно применять в любых сферах, а особенно в электронной коммерции; чем-то отдаленно такая технология напоминает старые бухгалтерские книги учета, только всё перенесено на электронные носители. Технология блокчейн приобрела за последнее время высокую популярность, а изначально она была создана исключительно для криптовалюты биткоин (рис. 3.3).

Информация, содержащаяся в блокчейне, существует как общая и постоянно согласованная база данных. База данных блокчейна не хранится в одном месте. Это означает, что сохраняемые записи действительно общедоступны и легко проверяемы.

– Нанотехнологии

Эта технология включает создание и манипулирование материалами размером от 1 до 100 нанометров, то есть материалами, близкими по размеру к молекулам, которые невозможно увидеть человеческим глазом.

С помощью этой технологии можно достичь наименьших размеров аппаратных средств, которых люди не могут достичь применяя другие технологии. К настоящему времени миллиарды долларов были вложены в исследования в области нанотехнологий. Цель состоит в том, чтобы использовать эти технологии для производства энергии, для создания материалов, в разработке оружия и, особенно, в медицине. Использование нанороботов для лечения болезней, которые до сих пор неизлечимы, лишь вопрос времени.

– Биотехнология

Биотехнология часто используется для борьбы с болезнями, уменьшая негативное воздействие человеческой деятельности на окружающую среду, улучшая производство продуктов питания и использование экологически чистой энергии. В настоящее время существует более 250 препаратов, разработанных благодаря использованию биотехнологии.

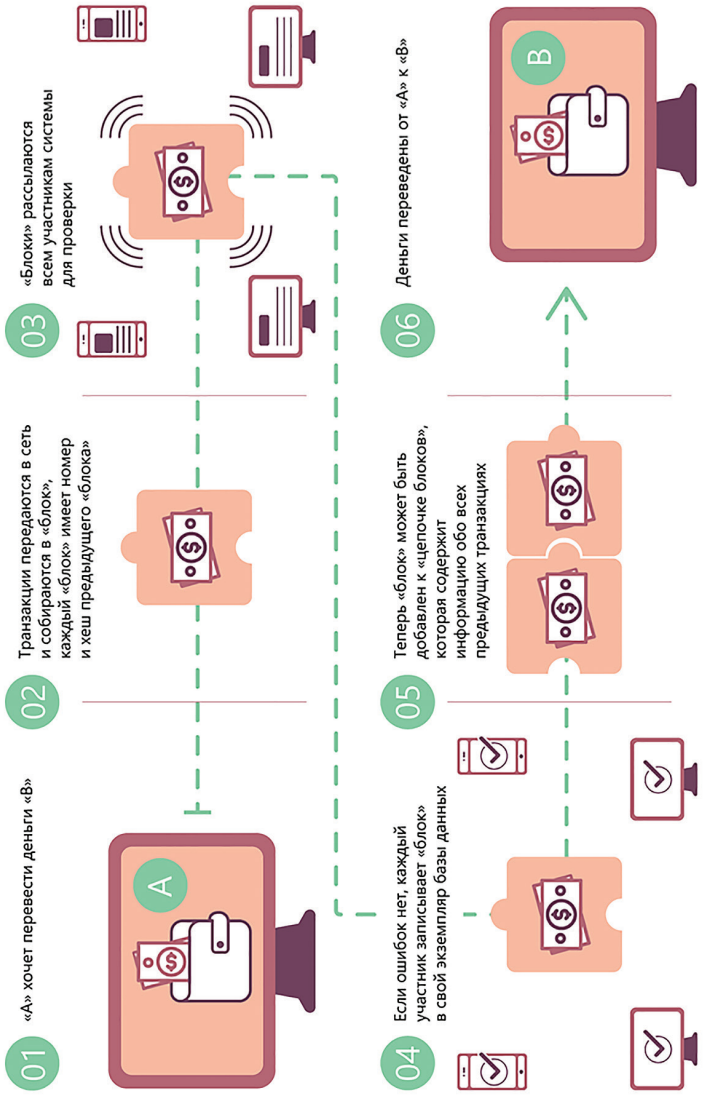


Рис. 3.3. Работа блокчейна на примере электронных денег

Компания, которая создает продукты с использованием биотехнологии, — Gilead Sciences. Её самый большой успех — это создание лекарства для борьбы с гепатитом С.

Также выдающимися в области биотехнологии являются такие компании, как Amgen (AMGN), основной продукт которой — противовоспалительный препарат Embrel, и компания CELG, которая стала известна, благодаря лекарству от язвы толстой кишки.

– Робототехника

Это отрасль машиностроения, которая сочетает в себе машиностроение, электротехнику и вычислительную технику. Целью этой технологии является создание автоматических машин, которые работают под контролем людей, чтобы выполнять действия, подобные человеческим, или выполнять действия, которые человек не может выполнять.

Сфера применения робототехники постоянно растет, ее используют как в военных целях, так и при выполнении некоторой работы по дому, для осуществления производственных операций и некоторых простых действий, которые могут быть автоматизированы.

Компания iRobot выпускает робототехнику: роботы-саперы, роботы-разведчики, робот-пылесос Roomba, моющий робот-пылесос Scooba.

Компания Google осуществляет сборку роботов. Компании Boston Dynamics и SCHAFT в настоящее время работают над улучшением автомобиля, которому не нужен будет водитель. Многие другие компании работают над созданием роботизированных моделей.

– Синтетическая биология

Синтетическая биология объединяет несколько дисциплин: генетика, молекулярная биология, молекулярная инженерия и биофизика. Её целью является создание искусственных организмов, которые могут выполнять полезные функции для человека.

Самой известной компанией, специализирующейся на этой технологии, является Intrexon, хотя есть также Gevo, Amyris или BioAmber.

– Датчики

Датчики из года в год облегчают жизнь человека. Функция этих устройств заключается в обнаружении изменений в физических или химических элементах. С их помощью можно измерить: интенсивность света, температуру, расстояние, ускорение, давление, крутящий момент, влажность, движение, PH и т. д.

Датчики помогают человечеству меньше тратить время на мониторинг, они считывают сигналы, которые испускают устройства. Они используются в медицине, в различных областях техники, для наблюдения, для безопасности людей и для улучшения здоровья.

Многие компании в настоящее время работают над тем, чтобы вывести на рынок самые функциональные датчики: инфракрасные, которые выполняют некоторые медицинские процедуры, датчики, которые превращают автомобили и промышленные машины в надежные устройства.

– Беспилотные летательные аппараты

Дроны — это самолеты, которые летают беспилотно и управляются дистанционном. Эти устройства обычно оснащены камерой и используются как для развлечения, так и для составления отчетов, в качестве инструмента наблюдения, для исследования районов, в которых человек подвергается большим рискам, для считывания информации с оборудования в труднодоступных для человека местах.

С 2010 года французская компания Parrot монополизировала продажу дронов благодаря своей модели ARdrone. Но в начале 2016 года китайская компания DJI переместила Parrot на второе место по продажам этих устройств.

Фантастические технологии, которые описывались в книгах и кино 10—20 лет назад, сегодня являются реальным фактом.

Настоящее выглядит многообещающе, что ждет нас в будущем?

– Квантовые вычисления

Квантовые вычисления — это вычисления на устройствах с использованием механических квантовых явлений (квантовая суперпозиция, квантовая запутанность) для передачи и обработки данных.

Квантовые компьютеры отличаются от двоичных цифровых электронных компьютеров, работающих на основе транзисторов.

В то время как обычные цифровые вычисления требуют, чтобы данные были закодированы в двоичных разрядах (битах), каждый из которых всегда находится в одном из двух определенных состояний (0 или 1), квантовый расчет использует квантовые биты.

Квантовый компьютер (в отличие от обычного) оперирует не битами (способными принимать значение либо 0, либо 1), а кубитами, имеющими значения одновременно и 0, и 1.

3.3. Наука о данных

Наука о данных (англ. data science) — это многодисциплинарная область, которая использует научные методы, процессы, алгоритмы и системы для извлечения знаний и идей из структурированных и неструктурированных данных. [18] Эта наука появилась в мире относительно недавно и только начинает набирать популярность в России. Как и любая другая наука, она имеет множество определений. Довольно точно и полно науку о данных определил в своей книге голландский учёный Вил ван дер Аалст. [9]

Наука о данных является междисциплинарной областью, направленной на превращение данных в реальную ценность. Данные могут быть структурированными или неструктурированными, большими или малыми, статиче-

скими или потоковыми. Ценность может быть обеспечена в виде прогнозов, автоматизированных решений, моделей, полученных из данных, или любого типа визуализации данных, предоставляющей информацию. Наука данных включает в себя извлечение данных, подготовку данных, исследование данных, преобразование, хранение данных, вычислительные инфраструктуры, различные виды майнинга и обучения, представление объяснений и прогнозов, а также использование результатов с учетом этических, социальных, юридических и деловых аспектов.

Приведенное выше определение подразумевает, что наука о данных шире прикладной статистики и интеллектуального анализа данных.

Люди, профессионально занимающиеся наукой о данных, называются специалистами по анализу данных или дата сайнтистами (data scientist). Специалисты по анализу данных помогают организациям превращать данные в ценную информацию, которая должна принести пользу компании. Эти специалисты могут ответить на множество вопросов, ответы на которые основаны на данных. Эти вопросы можно сгруппировать в следующие четыре основные категории:

– (Отчётность) Что случилось?
– (Диагностика) Почему это произошло?
– (Предсказание) Что произойдет?
– (Рекомендация) Что может быть лучше всего?

Наука о данных представляет собой объединение различных частично перекрывающихся (под)дисциплин. На рис. 3.4 показаны основные составляющие науки о данных. Дисциплины пересекаются друг с другом и различаются по объёму. Более того, границы не являются четкими и меняются со временем.

Сами данные, которые изучаются и анализируются, также играют огромную роль. Большие данные (англ. big data) — это область, в которой рассматриваются способы анализа и систематического извлечения информации из наборов данных, которые слишком велики или сложны

для обработки традиционными прикладными программами обработки данных. Данные с большим количеством строк обеспечивают большую статистическую мощность, в то время как данные с большей сложностью (больше атрибутов или столбцов) могут в то же время привести к ошибкам и ложным выводам. Основные сложности в использовании больших данных — это захват данных, хранение данных, анализ данных, поиск, обмен, передача, визуализация, запрос, обновление, конфиденциальность информации и источник данных. Большие данные традиционно связаны с ключевыми характеристиками: объем, многообразие, скорость и достоверность [11].

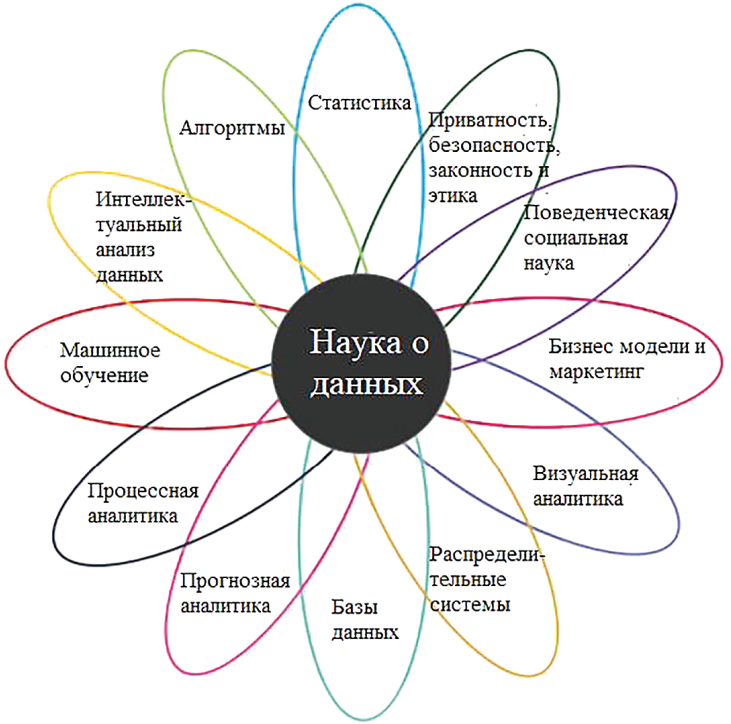


Рис. 3.4. Составляющие науки о данных

Большие данные можно описать следующими характеристиками [13]:

– Объем — количество генерируемых и хранимых данных. Размер данных определяет ценность и потенциальное понимание, а также могут ли эти данные считаться большими или нет.

– Многообразие — тип и характер данных. Это помогает людям, которые анализируют данные, эффективно использовать информацию, которую они вывели из этих данных. Большие данные получают из текста, изображений, аудио, видео.

– Скорость — в этом контексте, скорость, с которой данные генерируются и обрабатываются для удовлетворения потребностей и устранения проблем, которые лежат на пути роста и развития. Большие данные часто доступны в режиме реального времени. По сравнению с малыми данными, большие данные производятся с бóльшим постоянством. Два вида скорости, связанные с большими данными — это частота генерации и частота обработки, записи и публикации. [13]

– Достоверность — это расширенное определение для больших данных, которое относится к качеству данных и значению данных. Качество полученных данных может сильно варьироваться, влияя на точный анализ.

Данные должны быть обработаны с помощью передовых инструментов (аналитики и алгоритмов), чтобы выявлять действительно значимую информацию. [17]

Интеллектуальный анализ данных

Интеллектуальный анализ данных можно охарактеризовать как процесс поиска особенностей и интересной структуры в данных. Структура может принимать множество форм, включая набор правил, графики или сеть, одно или несколько уравнений и многое другое. Структура может быть частью сложной визуальной панели инструментов или просто как список политических кандидатов

и привязанный к ним номер, представляющий настроения избирателей на основе записей в Twitter.

В процессе интеллектуального анализа данных используется один или несколько алгоритмов для выявления интересных тенденций и закономерностей в данных. Знания, полученные в ходе этапа интеллектуального анализа данных, представляют собой обобщенную модель данных. Конечная цель — применить то, что было обнаружено, к новым ситуациям.

Существует несколько методов интеллектуального анализа данных. Однако все методы интеллектуального анализа данных используют индуктивное обучение. Индуктивное обучение — это процесс формирования общих определений понятий путем наблюдения конкретных примеров изучаемых понятий. [16]

Процесс интеллектуального анализа данных представляет собой конвейер, содержащий множество этапов — таких как очистка данных, извлечение функций и алгоритмическое проектирование.

Рабочий процесс типичной процедуры интеллектуального анализа данных содержит следующие этапы [14]:

1. Сбор данных. Сбор данных может потребовать использования:

– специального оборудования — такого как сенсорная сеть;

– ручного труда, такого как опросы пользователей;

– программных средств, таких как приложение для сбора веб-документов.

После этапа сбора данные часто хранятся в базе данных или в хранилище данных для обработки.

2. Извлечение признаков и очистка данных. Когда происходит сбор данных, они часто не подходят для последующей обработки. Например, данные могут быть закодированы в нераспознанные форматы. Во многих случаях различные типы данных могут произвольно смешиваться в документе свободной формы. Чтобы сделать данные пригодными для обработки, необходимо преобразовать их

в формат, дружественный алгоритмам интеллектуального анализа данных. Наиболее распространенным является многомерный формат, в котором различные поля данных соответствуют различным измеряемым свойствам, которые называются признаками, атрибутами или измерениями. Крайне важно извлечь соответствующие характеристики для процесса добычи. Этап извлечения признаков часто выполняется параллельно с очисткой данных, где недостающие и ошибочные части данных оцениваются или корректируются. Во многих случаях данные могут быть извлечены из различных источников и должны быть интегрированы в единый формат для обработки. Конечным результатом этой процедуры является красиво структурированный набор данных, который может эффективно использоваться компьютерной программой. После фазы извлечения признаков данные могут снова храниться в базе данных для обработки.

3. Аналитическая обработка и алгоритмы. Заключительной частью процесса анализа данных является разработка эффективных аналитических методов, на основе обработанных данных.

Общий процесс интеллектуального анализа данных показан на рис. 3.5. На первом этапе происходит сбор данных. Затем они обрабатываются путём извлечения важных признаков и очистки. Во время аналитического процесса данные преобразуются в готовые блоки, сформированные в удобном виде для последующего анализа аналитиками.

Рис. 3.5. Процесс интеллектуального анализа данных

Этап предварительной обработки или подготовки данных является, пожалуй, самым важным в процессе интеллектуального анализа данных. Этот этап начинается после сбора данных и состоит из следующих шагов:

1. Извлечение признаков: аналитик может столкнуться с огромными объемами необработанных документов, системных журналов или коммерческих транзакций без каких-либо указаний о том, как эти необработанные данные должны быть преобразованы в значимые функции базы данных для обработки. Эта фаза сильно зависит от аналитика, так как нужно понять, что именно будет влиять на результат анализа. Например, в приложении для обнаружения мошенничества с кредитными картами сумма сбора, частота повторения и местоположение часто являются хорошими показателями мошенничества. Однако многие другие признаки могут практически не являться показателями мошенничества.

2. Очистка данных: извлеченные данные могут иметь ошибочные или отсутствующие записи. Поэтому некоторые записи, возможно, потребуется удалить, или отсутствующие записи можно предположить или подставить на основе доступных похожих данных. Возможно, потребуется устранить несоответствия.

3. Выбор и преобразование признаков: когда данные очень многомерны, многие алгоритмы интеллектуального анализа данных не работают эффективно. Кроме того, многие признаки являются ошибочными по той или иной причине и могут добавлять ошибки в процесс интеллектуального анализа данных. Поэтому для удаления не относящихся к делу объектов или преобразования текущего набора объектов в новое пространство данных, более пригодное для анализа, используются различные методы.

Процесс очистки данных требует статистических методов, которые обычно используются для оценки недостающих данных. Кроме того, ошибочные записи данных часто удаляются для обеспечения более точных результатов интеллектуального анализа данных. Выбор и преобразо-

вание признаков не следует рассматривать как часть предварительной обработки данных, поскольку этап выбора признаков часто сильно зависит от конкретной решаемой аналитической задачи. В некоторых случаях процесс выбора признака может быть даже тесно интегрирован с используемым конкретным алгоритмом или методологией.

Машинное обучение

Машинное обучение — это обширная дисциплина, которая также входит в науку о данных. В разрезе машинного обучения изучается то, как системы учатся на данных. Системы могут быть обучены данными для принятия решений, и обучение является непрерывным процессом, в котором система постоянно поддерживает процесс обучения и улучшает свою способность принимать решения с большим количеством данных.

Машинное обучение является разновидностью искусственного интеллекта, который позволяет изучать и прогнозировать результаты без использования глубокого программирования. Термин «машинное обучение» часто используется вместо «искусственного интеллекта», потому что является его методом, который оказал наибольшее влияние на развитие этой сферы информационных технологий.

Крупные компании используют машинное обучение для принятия решений и автоматизации бизнес-процессов, изучая данные. Теперь простые в использовании инструменты, четко определенные алгоритмы и легкодоступные услуги представляют преимущества машинного обучения организациям любого размера. Компании, которые не используют машинное обучение для экономии на затратах, увеличения надежности и эффективности, вскоре будут вытеснены из конкурентной борьбы теми, кто внедряет эти технологии.

Вместо того чтобы писать алгоритмы и правила, которые принимают решения напрямую, или пытаться запрограммировать компьютер, чтобы он выполнял поставленные задачи, используя наборы правил, исключений и фильтров, машинное обучение учит компьютерные системы принимать решения, изучая большие наборы данных. Машинное обучение может создавать модели, которые представляют и обобщают шаблоны в данных, которые используются для такого обучения, и использовать эти модели для интерпретации и анализа новой информации.

В литературе существуют различные определения машинного обучения. Одно из них звучит так: «Область машинного обучения стремится ответить на вопрос “как мы можем построить компьютерные системы, которые автоматически улучшаются с опытом, и каковы фундаментальные законы, которые управляют всеми процессами обучения?» [17]

Спам-фильтр — хороший пример машинного обучения. По мере того, как ему передается больше данных, он продолжает подстраивать и адаптировать свои правила принятия решений под новые данные, используя методы машинного обучения, тем самым предотвращая получение спама в дальнейшем. Распознавание и подтверждение оплаты с помощью кредитных карт также основаны на нейронных сетях, еще одном популярном методе машинного обучения. Однако методы машинного обучения предпочитают данные суждениям, а наука о данных требует сбалансированного сочетания того и другого. Суждение необходимо для точной контекстуализации параметров анализа и построения эффективных моделей. Например, профессор статистики Винни Бразис, использует машинное обучение для прогнозирования доходов от кино. [14] Он утверждает, что простого машинного обучения будет недостаточно для получения точных предсказаний. Он дополняет машинное обучение суждениями, полученными из интервью со сценаристами, опросов и т. д., чтобы в результате получить более точный прогноз.

Машинный интеллект возрождается как новое воплощение искусственного интеллекта (область, которая, как многие считают, не оправдала ожиданий). Машинное обучение обещает и дает ответы на многие вопросы, представляющие интерес. Хилари Мейсон, основатель FastForwardLabs, специалист по Data Science в Accel, предлагает четыре характеристики машинного интеллекта, которые делают его интересным[9]:

1. Машинное обучение обычно основано на теоретическом прорыве и поэтому хорошо обосновано в науке.

2. Оно изменяет существующую экономическую парадигму.

3. Результатом машинного обучения является процесс перехода продукта из марочной категории в категорию рядовых продуктов за счет совершенствования производственных технологий (например, Hadoop).

4. Машинное обучение предоставляет новые данные, которые ведут к дальнейшему развитию науки о данных.

Машинное обучение отличается и теперь определяется отдельно от традиционной статистики. Машинное обучение больше касается обучения и сопоставления входных данных с выходными, в то время как в статистике всегда больше изучался анализ данных в рамках данной постановки проблемы или гипотезы. Машинное обучение, как правило, позволяет открывать что-то новое, в то время как эконометрика и статистический анализ, как правило, основаны на теории с жесткими предположениями. Машинное обучение имеет тенденцию фокусироваться больше на прогнозировании, которое даёт более полный результат, чем прогноз (или корреляция).

Домингос, ученый-практик, один из ведущих исследователей в области машинного обучения, в своём исследовании [12] рассматривает машинное обучение как сумму трёх компонентов: представления, оценки и оптимизации. Представление машинного обучения требует обозначения проблемы на формальном языке, который может обрабатываться с помощью компьютера. Эти представления будут отличаться для различных методов машинного обучения. Например, в задаче классификации может быть выбор многих классификаторов, каждый из которых будет формально представлен. Затем, чтобы завершить этап оценки, указывается функция подсчета очков или функция потерь. Наконец, наилучшая оценка достигается за счет оптимизации модели.

После того, как шаги были выполнены и наилучший алгоритм машинного обучения выбран из данных обучения, мы можем проверить модель на данных из выборки или набора тестовых данных. Можно случайным образом отобрать часть выборки данных для проверки. Повторение этого процесса путем предоставления различных частей данных для тестирования, а также обучение по остальным частям, является процессом, известным как перекрестная проверка, и настоятельно рекомендуется, чтобы достичь точных и объективных результатов.

Если окажется, что повторная перекрестная проверка приводит к плохим результатам, даже несмотря на то, что тестирование в образце работает очень хорошо, то это может свидетельствовать о чрезмерной подгонке. Чрезмерная подгонка обычно происходит, когда модель чрезмерно параметризована в выборке и подходит очень хорошо для конкретно данной выборки, но тогда она становится менее полезной для новых данных. Поэтому во многих случаях более простые и менее параметризованные модели, как правило, лучше работают при настройке параметров прогнозирования.

Машинное обучение по способу обучения делится на два типа: обучение с учителем, которое обучает модель известными входными и выходными данными, чтобы она могла предсказывать будущие результаты, и обучение без учителя, которое находит скрытые шаблоны или внутренние структуры во входных данных. Общая классификация методов машинного обучения показана на рисунке 3.6.

Алгоритм обучения с учителем принимает известный набор входных данных и известных значений для этих

данных (выход) и обучает модель генерировать разумные прогнозы (новые значения) для новых данных. Обучение с учителем используется, если известны данные для вывода, который необходимо предсказать.

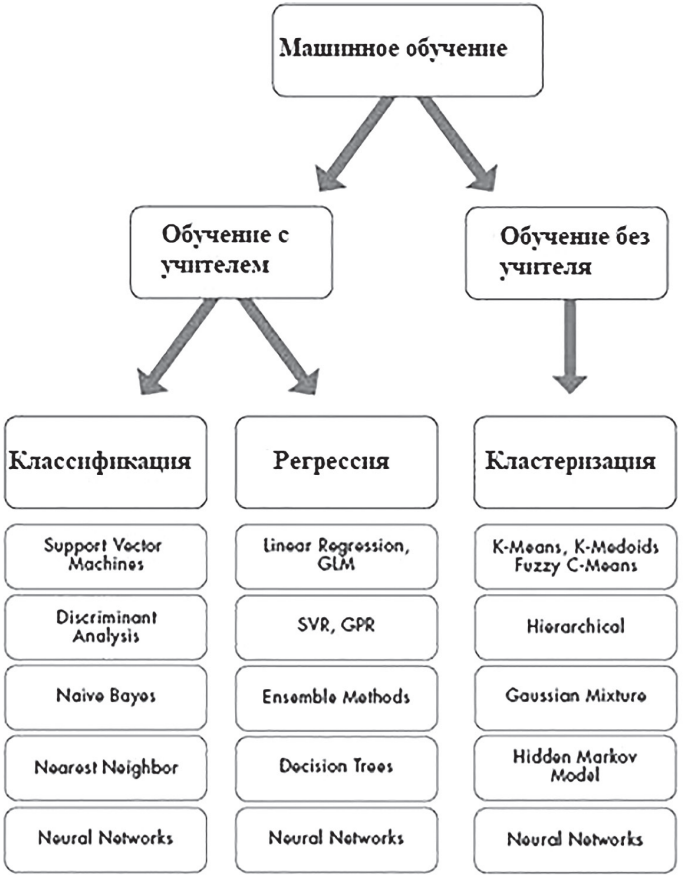


Рис. 3.6. Классификация методов машинного обучения

Контролируемое обучение использует методы классификации и регрессии для разработки прогностических моделей.

Методы классификации предсказывают дискретные ответы — например, является ли электронное письмо подлинным или спамом, или опухоль раковой или доброкачественной. Модели классификации классифицируют входные данные по категориям.

Общие алгоритмы для выполнения классификации включают в себя векторную машину поддержки, деревья решений, метод k-ближайших соседей, наивный байесовский классификатор, дискриминантный анализ, логистическую регрессию и нейронные сети.

Методы регрессии предсказывают непрерывные реакции — например, изменения температуры или колебания спроса на электроэнергию. Обычно применяются в прогнозировании нагрузки электричества и алгоритмической торговле.

Общие алгоритмы регрессии включают линейную модель, нелинейную модель, регуляризацию, ступенчатую регрессию, деревья решений, нейронные сети и адаптивную сеть на основе системы нечеткого вывода.

Обучение без учителя находит скрытые шаблоны или внутренние структуры в данных. Машинное обучение используется для построения выводов из наборов данных, состоящих из неопределённых входных данных.

Кластеризация является наиболее распространенным методом обучения без учителя. Она используется для исследовательского анализа данных для поиска скрытых шаблонов или групп в данных.

Общие алгоритмы для выполнения кластеризации включают метод k-средних, иерархическую кластеризацию, Гауссову смесь распределений, скрытые модели Маркова, самоорганизующиеся карты, метод нечёткой кластеризации C-средних и вычитающую кластеризацию.

Ансамбль моделей — это комбинации многих моделей машинного обучения. Существует много способов, с помощью которых модели могут быть объединены для создания лучших моделей. Но различные модели не всегда необходимы в решении одной определённой задачи.

Вместо этого можно откалибровать одну и ту же модель для разных подмножеств данных обучения, предоставляя несколько похожих, но разных моделей. Каждая из этих моделей затем используется для классификации вне выборки, и решение принимается путем отбора наиболее эффективных моделей. Этот метод известен как ***бэггинг***. Одним из наиболее популярных примеров алгоритмов бэггинга является модель случайного леса.

В другом методе — ***бустинге***, оптимизируемая функция потерь не взвешивает все примеры в наборе данных обучения одинаково. После одного прохода калибровки обучающие примеры взвешиваются таким образом, что случаи, когда алгоритм машинного обучения допустил ошибки (как в задаче классификации), получают более высокий вес в функции потерь. Подмечая эти наблюдения, алгоритм учится предотвращать эти ошибки, поскольку они являются более значимыми.

Другой подход к ансамблю методов называется ***стакинг***, когда модели прикованы друг к другу, так что выход данных низкоуровневых моделей становится входом другой модели более высокого уровня. Здесь модели интегрированы вертикально в отличие от бэгинга, где модели интегрированы горизонтально.

Наука о данных состоит из предсказаний и прогнозов. Но между ними есть разница. Статистик-экономист Пол Саффо предположил, что предсказания направлены на определение одного результата, в то время как прогнозы охватывают целый ряд результатов. Сказать, что «завтра будет дождь», — это сделать прогноз, но сказать, что «вероятность дождя составляет 40%» (подразумевает, что вероятность отсутствия дождя составляет 60%), — это значит сделать прогноз, поскольку он излагает диапазон возможных результатов с вероятностями. Делаются прогнозы погоды, а не предсказания. Предсказания — это утверждения большой определенности, в то время как прогнозы иллюстрируют диапазон неопределенности.

Глубокое обучение

Традиционные методы машинного обучения были ограничены в своей способности обрабатывать естественные данные в их сырой, необработанной форме. В течение десятилетий построение системы распознавания образов или машинного обучения требовало тщательного проектирования и значительного опыта в области разработки экстрактора объектов, который преобразовывал необработанные данные (например, значения пикселей изображения) в подходящее внутреннее представление или вектор объектов, из которого подсистема обучения может обнаруживать или классифицировать шаблоны во входных данных.

Обучение представлениям — это набор методов, в которых на вход подаются необработанные данные и затем автоматически обнаруживаются представления, необходимые для распознавания или классификации. Методы глубокого обучения — это методы представления-обучения с несколькими уровнями представления, полученные путем составления простых, но нелинейных модулей, каждый из которых преобразует представление на одном уровне (начиная с ввода сырых данных) в представление на более высоком, немного более абстрактном уровне. Благодаря такой структуре достаточно сложные функции могут быть извлечены. Для задач классификации более высокие уровни представления усиливают аспекты входных данных, которые важны для распознавания и подавляют нерелевантные вариации. Изображение, например, приходит в виде массива значений пикселей, и изученные объекты в первом слое представления обычно представляют наличие или отсутствие граней в системе координат изображения. Второй слой обычно обнаруживает рисунки, выделяя определенные расположения граней, независимо от небольших изменений в их положениях. Третий слой может собирать рисунки в более крупные комбинации, которые соот-

ветствуют частям знакомых объектов, а последующие слои будут обнаруживать объекты как комбинации этих частей. Ключевым аспектом глубокого обучения является то, что эти слои функций не разработаны инженерами-людьми: они извлекаются из данных с помощью процедуры обучения общего назначения.

Для анализа данных в глубоком обучении используются искусственные нейронные сети. Искусственная нейронная сеть (ИНС) — математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. [4] Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы.

ИНС основаны на наборе связанных единиц или узлов, называемых искусственными нейронами, которые свободно моделируют нейроны в биологическом мозге. Каждое соединение, подобно нейронам в биологическом мозге, может передавать сигнал от одного искусственного нейрона к другому. Искусственный нейрон, который получает сигнал, может обработать его, а затем сигнализировать дополнительным искусственным нейронам, связанным с ним.

В практических разработках сигнал в ИНС при связи между искусственными нейронами является вещественным числом, а выход каждого искусственного нейрона вычисляется некоторой нелинейной функцией суммы его входов. Связи между искусственными нейронами называются «гранями». Искусственные нейроны и края обычно имеют вес, который регулируется по мере обучения. Вес увеличивает или уменьшает силу сигнала при подключении. Искусственные нейроны могут иметь такой порог, что сигнал отправляется только в том случае, если совокупный сигнал пересекает этот порог. Как правило, искусственные нейроны объединяются в слои. Различные слои могут выполнять различные виды преобразований

на своих входах. Сигналы перемещаются от первого слоя (входного слоя) к последнему слою (выходному слою), иногда после многократного обхода слоев.

Первоначальная цель подхода ИНС состояла в том, чтобы решать проблемы так же, как это сделал бы человеческий мозг. Однако со временем внимание переключилось на выполнение конкретных задач, что привело к отклонениям от биологии. Искусственные нейронные сети используются для решения различных задач, включая компьютерное зрение, распознавание речи, машинный перевод, фильтрацию социальных сетей, в настольных и видеоиграх и в медицинской диагностике.

Глубокое обучение делает большие успехи в решении проблем, с которыми не справлялись методы искусственного интеллекта в течение многих лет. Оно оказалось очень хорошим инструментом для обнаружения сложных структур в многомерных данных и поэтому применимо ко многим областям науки, бизнеса и государства. В дополнение к тому, чтобы побить рекорды в распознавании изображений [7] и распознавании речи [5], глубокое обучение превзошло другие методы машинного обучения во многих аспектах науки, например, при прогнозировании активности молекул в наркотиках, анализе данных ускорителя частиц, реконструирующих схемы мозга, и предсказании влияния мутаций в некодирующей ДНК на экспрессию генов и болезни. Глубокое обучение дало весьма многообещающие результаты для решения различных задач в понимании естественного языка, особенно классификации конкретных тем, анализа настроений, ответов на вопросы и перевода на другой язык. [6]

3.4. Решение задач машинного обучения

Задача классификации сводится к распределению объектов выборки по n категориям на основании набора признаков. Следует отметить, что множество объектов, классовая принадлежность которых заранее известна,

называется обучающей выборкой. Решением задачи классификации называют построение алгоритма, способного классифицировать произвольный объект на основании множества признаков, классовая принадлежность которого заранее неизвестна. Примером задачи классификации может служить категоризация набора данных видов растений и животных на основании знаний, извлеченных из обучающей выборки.

Задача регрессии представляет собой прогнозирование некоторого числового значения, на основании набора признаков. Перед алгоритмом ставится задача построения функции $f : R^n \to R$. Принципиальное отличие этого класса задач от задачи классификации заключается в типе прогнозируемой переменной. Примерами задач регрессии являются прогнозирование цен акций на бирже ценных бумаг и прогнозирование выручки торговой точки в следующем периоде.

Задача кластеризации представляет собой распределение объектов выборки на основании набора признаков по n категориям, которые ранее не были определены. При решении задачи кластеризации алгоритм обрабатывает неразмеченный набор данных, разбивая выборку на непересекающиеся группы (кластеры). Примером задачи кластеризации может служить категоризация потребителей по степени заинтересованности группами товаров.

Задача выявления аномалий сводится к просмотру набора признаков, описывающих объекты выборки на предмет выявления нетипичного значения/сочетания значений одного или нескольких признаков. Примером задачи выявления аномалий являются задачи связанные с мониторингом состояния оборудования, подозрительной активности, связанной с нетипичными финансовыми операциями банковского счета.

Уменьшение размерности — это уменьшение числа признаков, описывающих объекты выборки. Согласно литературным данным, в некоторых случаях анализ данных, такой как регрессия или классификация, может быть осуществлён в редуцированном пространстве более точно, чем в исходном пространстве. [24]

Для решения вышеперечисленных задач применяются различные аналитические алгоритмы: Деревья принятия решений, случайный лес, KNN (метод k ближайших соседей), линейная и логистическая регрессии, метод опорных векторов, PCA (метод главных компонент), ICA (анализ независимых компонент), сингулярное разложение, CART и многие другие.

Методы машинного обучения «с учителем»

Алгоритмы машинного обучения «с учителем» решают аналитические задачи, которые подразумевают необходимость наличия обучающей выборки. Обучающей выборкой в данном случае является размеченный набора данных, для которого заранее известна целевая переменная (прогнозируемый параметр). Задача обучения «с учителем» сводится к задаче ассоциации некоторого «ввода» с некоторыми вариантами «вывода». Примером такой задачи может служить задача построения модели классификации растений, обученной на основании обучающей выборки, в которой каждый случай измерений заранее ассоциирован с конкретным видом растения.

Методы машинного обучения «без учителя»

Алгоритмы машинного обучения «без учителя» решают аналитические задачи, связанные с изучением структуры и свойств собранного набора данных. Такой набор данных является неразмеченным, другими словами, в нем отсутствуют данные о целевой переменной.

Деревья принятия решений

Деревья принятия решений представляют собой логические схемы, которые позволяют получить конечный результат классификации объекта с помощью набора отве-

тов на иерархически организованную систему вопросов. Структура дерева решений содержит 2 класса объектов: листья и ветви. Листья дерева решений содержат в себе условия для значений переменных, описывающих отдельный объект классификации. Листья дерева решений могут быть внутренними и терминальными. Внутренние вершины содержат предикаты, позволяющие направить объект классификации по соответствующей ветви. Терминальные вершины содержат в себе конечную метку класса. Пример решающего дерева представлен на рис. 3.7.

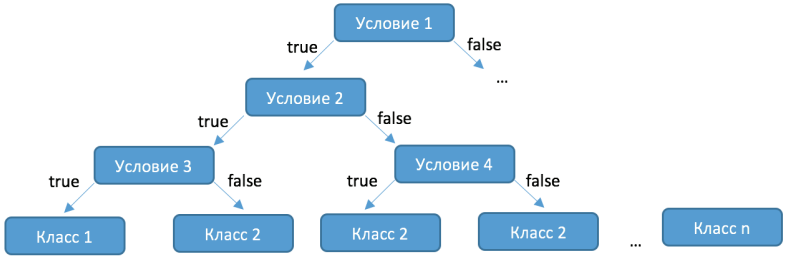


Рис. 3.7. Структура решающего дерева

Информационная энтропия представляет собой меру неопределённости некоторой системы (в статистической физике или теории информации), в частности непредсказуемости появления какого-либо символа алфавита. В последнем случае уровень энтропии численно равен количеству информации на символ передаваемого сообщения. [25]

Функция энтропии Шеннона имеет вид:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i ,$$

где p_i — это вероятность нахождения системы в i-ом состоянии. Следует отметить, что чем выше уровень энтропии H, тем ниже уровень упорядоченности в системе. Таким образом, перед аналитическими алгоритмами ставится задача минимизации функции энтропии.

При прогнозировании качественного признака (задача классификации) алгоритм построения дерева решений включает в себя следующие шаги:

– расчёт уровня энтропии исходной выборки;

– перебор возможных условий первого листа дерева решений (для каждого элемента выборки необходимо перебрать все его атрибуты и сгенерировать предикат, способный разделить выборку);

– расчёт нового уровня энтропии системы при разделении выборки на основании каждого предиката;

– выбор предиката, при котором будет наблюдаться максимальное снижение уровня энтропии;

– повторение предыдущих шагов рекурсивно до тех пор, пока в каждой из подвыборок не окажутся объекты одного класса.

В случае прогнозирования количественного признака (задачи регрессии) используется другая метрика оценки прироста упорядоченности при разбиении выборки, так называемая дисперсия вокруг среднего:

$$D = \frac{1}{l}\sum_{i=1}^{l}(y_i - \frac{1}{l}\sum_{i=1}^{l} y_i)^2 .$$

Таким образом, алгоритм построения дерева решений при решении задачи регрессии будет выполняться до того момента, пока в каждой из подвыборок не окажутся объекты со значением целевой переменной в допустимом диапазоне.

Пример расчёта уровня энтропии системы и построения дерева решений

Построим дерево решений (рис. 3.8).

KNN (Метод k ближайших соседей)

Метод k ближайших соседей — это алгоритм, который применяется в решении задач классификации и регрессии. KNN основывается на гипотезе компактности.

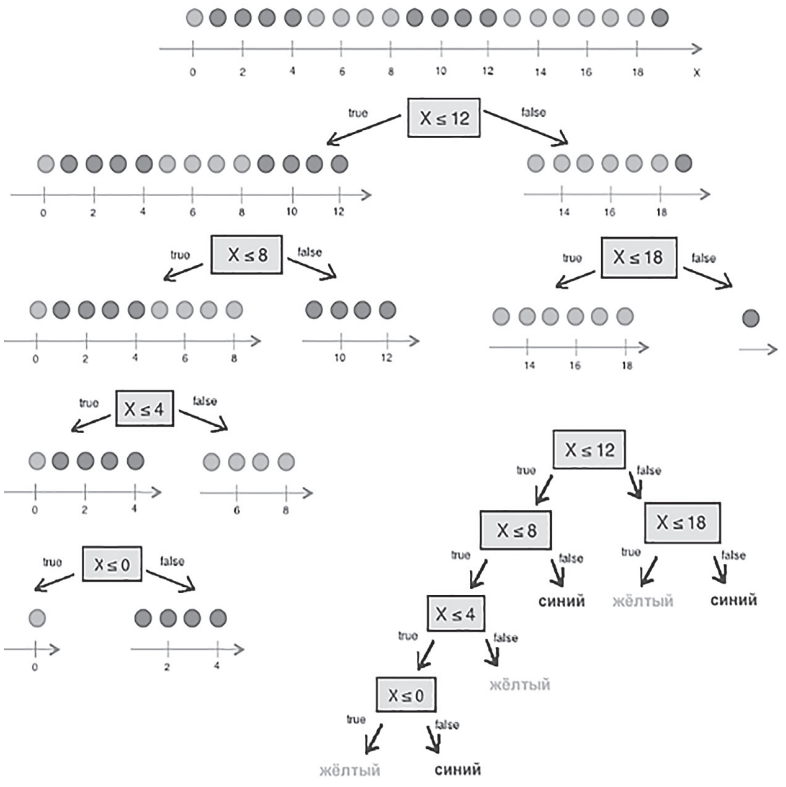


Рис. 3.8. Дерево решений

Гипотеза компактности — это предположение о том, что схожие объекты гораздо чаще лежат в одном классе, чем в разных; или, другими словами, что классы образуют компактно локализованные подмножества в пространстве объектов. Из вышесказанного также можно сделать вывод, что граница между классами имеет достаточно простую форму. [26]

Пусть задана обучающая выборка пар «объект-ответ»

$$X^m = \{(x_1, y_1), \ldots, (x_m, y_m)\}$$

Пусть на множестве объектов задана функция расстояния $p(x, x_m)$. Задачей этой функции является отображение степени сходства/различия между объектами выборки. Таким образом, значение функции расстояния между объектами обратно пропорционально степени схожести объектов выборки.

Первым этапом реализации метода ближайших соседей является выбор адекватной задаче метрики расстояния и расчёт расстояний между объектами выборки. Для расчёта меры расстояния между объектами выборки используют следующие метрики: евклидово расстояние, квадрат евклидова расстояния, манхэттенское расстояние, степенное расстояние и др.

Евклидово расстояние $d(p,q)$ для точек $p = (p_1, \ldots, p_n)$ и $q = (q_1, \ldots, q_n)$ рассчитывается по формуле:

$$d(p,q) = \sqrt{\sum_{k=1}^{n} (p_k - q_k)^2}$$

Квадрат евклидова расстояния:

$$d(p,q) = \sum_{k=1}^{n} (p_k - q_k)^2$$

Манхэттенское расстояние:

$$d(p,q) = \sum_{k=1}^{n} |p_k - q_k|$$

Степенное расстояние:

$$d(p,q) = \left(\sum_{k=1}^{n} |p_k - q_k|^b\right)^{\frac{1}{r}}$$

где b и r это параметры настройки модели, определяемые пользователем.

После выбора метрики и расчёта расстояний необходимо отсортировать объекты выборки по возрастанию значения функции расстояния $p(x, x_m)$ до классифициру-

емого объекта. Таким образом, алгоритм классификации KNN включает в себя следующие шаги:

– нормализация данных;

– вычисление расстояний между объектами выборки;

– сортировка объектов выборки по убыванию значения функции расстояния $p(x, x_m)$;

– присвоение анализируемому объекту класс, наиболее часто встречающийся среди k соседей.

Одним из механизмов настройки работы алгоритма классификации KNN является перебор параметра k (количество k соседей). При $k = 1$ алгоритм ближайшего соседа является неустойчивым к шумовым выбросам. [27] При $k = m$, степень устойчивости предельно растет и результат работы алгоритма превращается в константу. Учитывая вышеперечисленное, можно сделать вывод о том, что оптимальное значение параметра k отличается от крайних значений $k = 1$ и $k = m$, где m количество элементов выборки. Для подбора оптимального параметра k используют алгоритм кросс-валидации.

Кросс-валидация — это группа методов оценки качества предиктивной модели, которые основываются на перекрестном разбиении первичной выборки на обучающие и тестовые наборы данных и получении усредненного результата по всем случаям разбиения. Схема перекрестного разбиения набора данных представлена на рисунке 3.9.

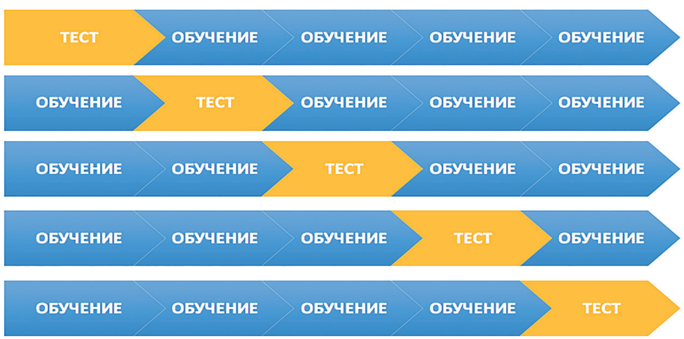


Рис 3.9. Схема кросс-валидации

Кросс-валидация позволяет осуществлять более взвешенный выбор архитектуры модели анализа данных, однако является ресурсоемкой операцией, сложность которой резко возрастает с увеличением объема, анализируемых данных.

Нормализация данных является необходимым этапом подготовки данных в тех случаях, когда поля различных признаков содержат данные в разных единицах измерения. Если не производить нормализацию данных, признаки, значения которых находятся в диапазоне от 0 до 100, окажут большее влияние на целевую переменную, чем признаки, значения которых находятся в диапазоне от 0 до 10. Нормализация величины x_j производится по формуле:

$$x_j \equiv \frac{x_j - x_{min}}{x_{max} - x_{min}}.$$

Результатом нормализации является набор данных, значения признаков которого варьируются в диапазоне от 0 до 1 и таким образом содержит относительные величины вместо абсолютных. Вышеописанная операция позволяет нивелировать влияние признаков.

Пример нормализации данных и классификации нового наблюдения методом k ближайших соседей.

В таблице представлен классифицированный (размеченный) набор данных о наблюдениях, собранных по двум признакам, значения которых варьируются от 0 до 1000 для первого признака и от 0 до 10 для второго. Проведем классификацию Наблюдения 19 со значениями признаков:

Признак 1 — 90

Признак 2 — 1,3

Наблюдение №	Признак 1	Признак 2	Класс
1	100	0,9	1
2	80	1,1	1

Окончание таблицы

Наблюдение №	Признак 1	Признак 2	Класс
3	80	0,9	1
4	180	0,8	3
5	80	1,6	2
6	170	1	3
7	180	1,1	3
8	160	1,1	3
9	70	0,8	1
10	100	1,4	2
11	90	1,5	2
12	110	1,7	2
13	60	1	1
14	190	1	3
15	180	0,9	3
16	80	0,7	1
17	100	1,6	2
18	110	1,5	

Шаг 1. Нормализация данных

Произведем нормализацию набора данных, после чего значения признаков будут варьироваться в диапазоне от 0 до 1 и таким образом содержать относительные величины вместо абсолютных.

Нормализация значений признаков наблюдения 1:

Нормализация признака 1:

$$X_1^1 = \frac{100-0}{1000-0} = 0{,}1$$

Нормализация признака 2:

$$X_1^2 = \frac{0{,}9-0}{10-0} = 0{,}09$$

Нормализованные значения признаков запишем в таблицу:

Наблюдение №	Признак 1	Признак 2	Класс
1	0,1	0,09	1
2	0,08	0,11	1
3	0,08	0,09	1
4	0,18	0,08	3
5	0,08	0,16	2
6	0,17	0,1	3
7	0,18	0,11	3
8	0,16	0,11	3
9	0,07	0,08	1
10	0,1	0,14	2
11	0,9	0,15	2
12	0,11	0,17	2
13	0,06	0,1	1
14	0,19	0,1	3
15	0,18	0,09	3
16	0,08	0,07	1
17	0,1	0,16	2
18	0,11	0,15	2

Шаг 2. Нормализация значений признаков нового наблюдения

Произведем нормализацию значений признаков нового наблюдения согласно их диапазонам.

Нормализация значений признаков наблюдения 19:

Нормализация признака 1:

$$X_{19}^1 = \frac{90-0}{1000-0} = 0{,}09$$

Нормализация признака 2:

$$X_{19}^2 = \frac{1,3-0}{10-0} = 0,13$$

Шаг 3. Сортировка объектов выборки по убыванию значения функции расстояния

Ниже приведён расчёт расстояния между Наблюдением 1 и Наблюдением 19:

$$d(1,19) = \sqrt{(0,1-0,09)^2 + (0,09-0,13)^2} = \\ = 0,0412310562561766.$$

Рассчитаем расстояния до других наблюдений и запишем их в таблицу, округлив до 4-х знаков после запятой, а затем отсортируем получившийся массив по возрастанию расстояния до классифицируемого наблюдения:

Наблюдение №	Класс	Расстояние
10	2	0,0141
2	1	0,0224
18	2	0,0283
5	2	0,0316
17	2	0,0316
1	1	0,0412
3	1	0,0412
13	1	0,0424
12	2	0,0447
9	1	0,0539
16	1	0,0608
8	3	0,0728
6	3	0,0854
7	3	0,0922

Окончание таблицы

Наблюдение №	Класс	Расстояние
15	3	0,0985
4	3	0,103
14	3	0,1044
11	2	0,8102

Шаг 4. Определение числа k соседей

На этом шаге необходимо выбрать число соседей и определить, к какому классу принадлежит большинство из них.

Если $k = 1$, то ближайшим соседом будет Наблюдение 10 и результатом классификации будет Класс 2.

Если $k = 2$, то Наблюдение 19 будет классифицировано в Класс 2 и Класс 1 с равной долей вероятности.

При $k = 4$ результатом классификации является Класс 2.

Таким образом, очевидно, что результат классификации сильно зависит от значения параметра k. При выборе слишком малого значения k присутствует риск того, что ближайшими соседями классифицируемого наблюдения окажутся выбросы. В таком случае результат классификации окажется неверным. Существует возможность минимизировать подобный риск ограниченным увеличением числа соседей. В случае, когда выбрано максимальное количество соседей $k = N$, где N это общее количество наблюдений выборки, классифицируемому объекту будет присваиваться наиболее часто встречающийся класс, результат алгоритма превратится в константу для данной выборки. Обычно значение параметра k может варьироваться от 3 до 10 и часто оказывается близким к квадратному корню от числа всех наблюдений выборки. [28] Оптимизация числа соседей достигается перебором значений параметра k на тестовых выборках при кросс-валидации.

Метрики качества

Для сравнения эффективности применения различных алгоритмов машинного обучения существует необходимость определения метрики качества, которые могут выступить в качестве индекса производительности P для задач класса T. [21]

Классическими метриками качества для задач регрессии являются средняя абсолютная (Mean Absolute Error, MAE) и средняя квадратичная ошибки (Mean Squared Error, MSE).

$$MAE = \frac{1}{l}\sum_{i=1}^{l}\left(a\left(x_i\right) - y_i\right)^2$$

$$MSE = \frac{1}{l}\sum_{i=1}^{l}\left|a\left(x_i\right) - y_i\right|^2$$

Описание метрик качества для задач классификации требует представления следующей концепции для описания этих метрик в терминах ошибок классификации, которые в англоязычной литературе именуются как confusion matrix (матрица неточностей). Рассмотрим пример: допустим, что у нас есть два класса и алгоритм, предсказывающий принадлежность каждого объекта одному из классов, тогда матрица ошибок классификации будет выглядеть следующим образом [26]:

	$y = 1$	$y = 0$
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)
$\hat{y} = 0$	False Negative (FN)	True Negative (TN)

Здесь $\hat{y}$ — это ответ алгоритма для данного объекта, а y — истинная метка класса на этом объекте;

TP — True Positive — доля правильных прогнозов «попадание»;

TN — True Negative — доля случаев, при которых модель разумно проигнорировала объекты выборки;

FP — False Positive — доля ложных прогнозов «ложная тревога»;

FN — False Negative — доля случаев, при которых модель проигнорировала объекты, действительно относящиеся к искомому классу «пропуск цели».

Точность (Preceision)

$$\text{Preceision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

Точностью работы алгоритма в данном случае является доля правильно классифицированных объектов выборки от общего числа случаев классификации.

Полнота (Recall)

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

Полнотой работы алгоритма является доля правильно классифицированных объектов выборки от общего числа объектов, действительно находящихся в целевом классе.

F-мера (F-measure)

$$\text{F} - \text{measure} = \frac{2 * \text{Preceision} * \text{Recall}}{\text{Preceision} + \text{Recall}}$$

F-мера является гармоническим средним показателей точности и полноты.

Accuracy

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

Мера Accuracy представляет собой консолидированный показатель точности работы модели по всем классам.

Пример расчета качества работы алгоритма классификации

Пусть из 10100 единиц эксплуатируемого оборудования откажет 100 единиц и есть алгоритм, правильно предсказывающий 90 отказов. Построим матрицу неточностей:

	Факт: откажет	Факт: не откажет
Прогноз: откажет	90	30
Прогноз: не откажет	30	9950

Точность (Preceision)

$$\text{Preceision} = \frac{90}{90+30} = 0,9$$

Полнота (Recall)

$$\text{Recall} = \frac{90}{90+30} = 0,9$$

F-мера (F-measure)

$$\text{F} - \text{measure} = \frac{2*0,9*0,9}{0,9+0,9} = 0,9$$

Accuracy

$$\text{Accuracy} = \frac{90+9950}{90+9950+30+30} \approx 0,95$$

Вопросы для самоконтроля

1. Назовите способы создания ресурсов в облаке.
2. Определите безопасность облачных ресурсов.
3. Назовите способы и методы обработки больших данных.
4. В чем отличие в основных типах архитектуры традиционных информационных систем: монолитной, многослойной, архитектуры микросервисов, общей структуры масштабируемой системы, на основе кластера, Event-driven?
5. Назовите признаки бессерверной архитектуры.
6. Назовите признаки и свойства облачных хранилищ AWS.

7. Чем отличается реляционная база данных от нерялиционной?.
8. Сформулируйте основные возможности облачного сервеса AWS RDS — Amazon Web Services Relational Database Service.
9. Сформулируйте подходя, реализуемые в нереляционных базах данных.
10. Сделайте сравнительный анализ реляционных хранилищ данных: Azure SQLDWH, AWS RedShift.
11. Определите возможности специализированных облачных хранилищ больших данных.
12. Назовите облачные сервисы копирования и трансформации данных с их основными признаками, характеристиками.
13. Назовите параметры, свойства, характеристики интерактивного анализа данных.
14. Как осуществляется организация автоматического индексирования документов в сервисе Cosmos DB?
15. Определите принципы организации потокового анализа данных в системах: Azure Stream Analytics, Amazon Kinesis Analytics, Apache Storm.
16. Как вы думаете, какие еще технологии повлияют на будущее?

Список использованных источников главы 3

1. Алексеева В. А. Использование методов машинного обучения в задачах бинарной классификации [Текст] // Математическое моделирование. — 2015. — № 3(41). — С. 58—63.

2. Барсегян А. А. Технологии анализа данных. Data Mining, Visual Mining, Text Mining, OLAP [Текст] / А.А Барсегян. и др. — СПб.: БХВ-Петербург, 2016. — 384 с.

3. Галимов Р.Г Основы алгоритмов машинного обучения — обучение с учителем [Текст] // Научно-практи-

ческий электронный журнал Аллея Науки. — 2017. — №14. — С. 1—10.

4. Гудфеллоу Я. Глубокое обучение [Текст] / Я. Гудфеллоу, И. Бенджио, А. Курвилль. — М.: ДМК, 2018. — 564 с.

5. Иконникова О. И. Новые возможности маркетинга в эпоху больших данных и машинного обучения [Текст] // Экономика и бизнес: теория и практика. — 2017. — №5. — С. 105—108.

6. Лагутаева Д. А. Влияние маркетинговых практик на прибыльность компаний: исследование методом машинного обучения [Текст] / Д. А. Лагутаева, О. А. Третьяк, А. Ю. Григорьев // Российский журнал менеджмента. — 2016. — № 14(4). — С. 3—20.

7. Мельников Э. А. Машинное обучение в маркетинге финансовых продуктов [Текст]: тез. Докл. 1-й Международной научно-практической конференции. — М., 2017. — С. 148.

8. Мокшин В.В и др. Распознавание образов транспортных средств на основе эвристических данных и машинного обучения [Текст] / В. В. Мокшин, И. Р. Сайфудинов, А. П. Кирпичников, Л. М. Шарнин // Вестник Казанского технологического университета. — 2016. — № 5. — С. 130—137.

9. Николенко С. И. Глубокое обучение [Текст] / С. И. Николенко, А. А. Кадурин, Е. О. Архангельская. — СПб.: Питер, 2018. — 481 с.

10. Рассохина Е. Д. Применение методов машинного обучения в цифровом маркетинге / Е. Д. Рассохина, Е. В. Сумарокова [Текст] // Государственный университет управления. — 2017. — №4. — С. 32—37.

11. Шмид А. В. Машинное обучение в экспертных системах: подготовка специалистов [Текст] / А. В. Шмид, К. А. Лычагин // Образовательные ресурсы и технологии. — 2014. — № 2(5). — С. 102—106.

12. Aggarwal C. C. Data Mining: The Textbook [Текст]. — Springer, 2015. — 734 p.

13. Asir Antony Gnana Singh D., Machine Learning based Business Forecasting [Текст] / D. Asir Antony Gnana Singh, E. Jebamalar Leavline, S. Muthukrishnan, R. Yuvaraj // International Journal of Information Engineering and Electronic Business. — 2018. — № 6. — С. 40—51.

14. Automatic Differentiation in Machine Learning: a Survey [Текст] / A. G. Baydin и др. // Journal of Machine Learning Research. — 2018. — № 18. — С. 1—43.

15. Boadway R. The economic evaluation of projects [Текст] // Queen's University, Kingston, Canada. — 2019. — № 2. — P. 18—22.

16. Bohanec M. Explaining machine learning models in sales predictions [Текст] / M. Bohanec, M. K. Borštnar, M. Robnik-Šikonja // Expert Systems with Applications. — 2017. — № 71. — С. 416 -428.

17. Bohanec M. Integration of Machine Learning Insights into Organizational Learning: A Case of B2B Sales Forecasting. [Текст] / Bohanec, M. K. Borštnar, M. Robnik-Šikonja // Blurring the Boundaries Through Digital Innovation. — 2016. — № 9. — С. 23—28.

18. Bottou L. Optimization Methods for Large-Scale Machine Learning [Текст] / L. Bottou, F. E. Curtis, J. Nocedal // Society for Industrial and Applied Mathematics. — 2018. — № 60. — С. 223—311.

19. https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning/

20. Samuel Arthur L. (1959). Some Studies in Machine Learning Usinthe Gameof Checkers. // IBM Journal of Research and Development. 44: 206—226.

21. Machine Learning Tom M. Mitchell 432 pages McGraw-HillScience/Engineering/Math; (March 1, 1997).

22. П Флах. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. — М.: ДМК, 2015. — 402 с.

23. Antonio Rico-Sulayes. Reducing Vector Space Dimensionality in Automatic Classification for Authorship Attribution // Revista Ingeniería Electrónica, Automática y Comunicaciones. – 2017. – Т. 38, № 3. с. 26—35.

24. https://habr.com/ru/company/ods/blog/328372/ (дата обращения: 07.02.2020).

25. https://ru.wikipedia.org/wiki/Информационная_энтропия (дата обращения: 07.02.2020).

26. http://www.machinelearning.ru/wiki/index.php?title=%D0%93%D0%B8%D0%BF%D0%BE%D1%82%D0%B5%D0%B7%D0%B0_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BA%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения: 07.02.2020).

27. http://www.machinelearning.ru/wiki/index.php?title=KNN (дата обращения: 07.02.2020).

28. Brett Lantz. Machine Learning with R. Pack Publishing. — Birmongham-Mumbai, 2013. (дата обращения: 07.02.2020).

Глава 4
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

XXI век — век цифровой экономики с интенсификацией производственных структур и общественных отношений. Происходящие производственные процессы уже невозможно представить без использования современных цифровых технологий. Возрастающие объемы информации, которые проходят стадии передачи, обмена, обработки, хранения опираются на новейшие нанотехнологии, информационно-телекоммуникационные сети, программно-аппаратное обеспечение. Компьютеризация и глобальные вычислительные сети, новейшие информационные технологии создают для информационной среды все более новые источники угроз. Владея информацией, особенно если она обременена ценностью, немаловажной задачей становится ее защита. Темпы развития современных информационных систем и технологий опережают темпы развития средств, обеспечивающих информационную защиту.

Незащищенность информации от искажения, нарушения целостности, кражи, потери может нанести непоправимый урон любому субъекту или объекту цифровой экономики. Особенно это касается таких сфер, как оборона, военно-промышленный комплекс, космические разработки, медицина, финансы, банки и т. д. В настоящее время особый интерес уделяется проблеме кибербезопасности. Именно киберпреступления реально угрожают цифровой экономике на любом ее участке и стадии развития.

Решение данной проблемы, ставшей уже мировой, невозможно осуществить силами только одного государства из-за ограниченности ресурсов. Данную задачу можно решить только усилиями международного сотрудничества.

4.1. Предмет и объект защиты

Организация защиты информации — это первостепенная и животрепещущая задача. Информация присутствует во всех сферах нашей деятельности.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ (принят Государственной Думой 8 июля 2006 года), говорится, что «**информация** — сведения (сообщения, данные) независимо от формы их представления» [1].

Информация, подлежащая защите — это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственниками информации при ее передаче, обработке и хранении в компьютерных системах и сетях.

В качестве **объекта** защиты информации выступают компьютерные системы (КС), информационные ресурсы, информационные системы и технологии, нормативные документы, архивы, обслуживающий персонал, а также здания и помещения. В понятие КС входят ЭВМ, вычислительные комплексы, системы и сети. Взаимосвязь объектов и субъектов в обеспечении защиты информации рассматривается в международном стандарте ISO/IEC-15408 (принят в России как ГОСТ Р ИСО/МЭК 15408—2002).

Собственниками или **субъектами** информации могут быть государство, а также юридические (организации, предприятия, фирмы) и физические лица [1].

Информация обладает определенными свойствами (см. рис. 4.1).

Информация достоверна, если в неё не внесены какие-либо искажения, и она отражает фактическое состояние дел.

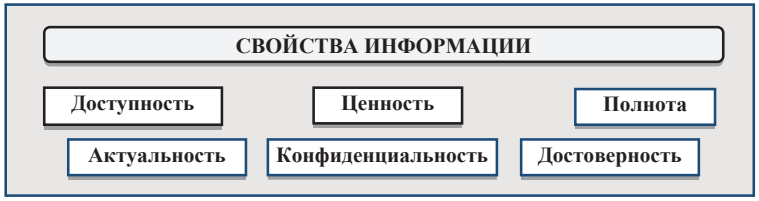


Рис. 4.1. Свойства информации

Если информация в полной мере отвечает (отражает) текущему моменту времени, то она считается актуальной. Действия, направленные на нарушение полноты, целостности информации, выраженное в ее изменении или уничтожении, рассматриваются с учетом легальности и регламентируются правилами политики безопасности. «Политика безопасности — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности» [10].

Основным документом для проведения политики информационной безопасности на предприятии является программа информационной безопасности, в которой содержатся цели, требования, основные направления решения задач, связанных с построением системы защиты информации. Для этого необходимо иметь информацию, описывающую структуру предприятия со всеми подразделениями и персоналом, их функциональные связи, информационные объекты, технические и программные средства, средства телекоммуникаций и т. д.

Под безопасностью информации понимается обеспечение ее целостности, доступности и конфиденциальности.

Информация сегодня — это не только ценный товар, но она также является стратегическим оружием. Ценность информации зависит от времени и определяется степенью (уровнем) ее полезности для владельца (субъекта).

Ценность информации со временем уменьшается. Зависимость ценности информации от времени приближенно определяется по формуле:

$$\tilde{N}(t) = C_0 e^{-2,3t/\tau},$$

где C_0 – ценность информации в момент ее возникновения (получения);

t — время от момента возникновения информации до момента определения ее стоимости;

τ — время от момента возникновения информации до момента ее устаревания.

Наглядно такая зависимость отображена на графике (см. рис. 4.2):

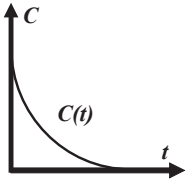


Рис. 4.2. Изменение ценности информации во времени

Информация полная, если она отвечает всем требованиям, на основании которых можно принимать те или иные решения.

Информация является конфиденциальной, когда субъект, получивший доступ к ней, не обладает правом передачи ее другому субъекту без согласования с ее обладателем. «Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам» [2]. Конфиденциальная информация также может содержать государственную или коммерческую тайну (см. рис. 4.3).

В сферу коммерческой тайны входят такие сведения, как информация о финансовой деятельности предприятия/организации, о производстве и производимой продукции, о научных исследованиях и разработках, о методах управления, о сотрудниках предприятия и т. д.

Делая акцент на информации, нельзя не говорить сегодня о таком понятии, как информационные ресурсы,

представляющие собой массивы данных, документы, библиотеки, архивы, банки и базы данных в автоматизированных системах. В состав автоматизированной системы входят технические, программные, информационные ресурсы. Согласно определению ГОСТа, «*угроза* (безопасности информации) — совокупность условий и факторов, создающих потенциальную и реально существующую опасность нарушения безопасности информации» [13]. Причиной возникновения угрозы безопасности может быть субъект, материальный объект, физическое явление. Примерами угроз в компьютерных сетях (КС) могут быть преднамеренные и непреднамеренные действия пользователя: несанкционированный доступ (НСД) к информации (т. е. доступ к информации субъекта (лица), не наделённого соответствующими правами) с дальнейшими такими действиями, как кража, уничтожение, модификация, искажение, разглашение, а также непредвиденные обстоятельства — пожары, наводнения, нарушения в электроснабжении, ошибки в эксплуатации, сбои и отказы оборудования и т. д. (см. рис. 4.4).

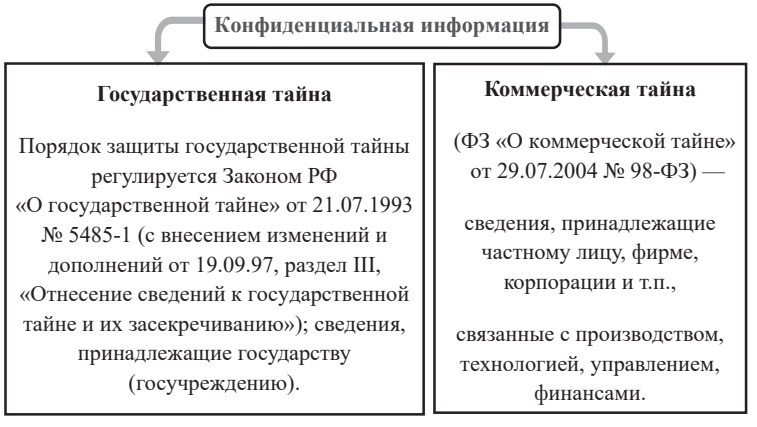


Рис. 4.3. Разновидности конфиденциальной информации

Рис. 4.4. Угрозы безопасности информации в КС

4.2. Методы и средства защиты информации

Защита информации требует комплексного подхода с использованием средств, методов и мероприятий с целью обеспечения более высокой степени надежности информации, подвергающейся обработке, передаче, хранению, накоплению. К основным методам защиты относятся:

Препятствие — физическая защита информационных систем и средств автоматизации от проникновения злоумышленников на охраняемый объект.

Управление — процессы управления всеми средствами защиты данных и компонентов вычислительных систем.

Маскировка — процесс переработки данных с использованием их преобразования методами криптографии. Особенно это актуально при передаче информации по каналам связи.

Регламентация — разработка и реализация методов защиты информационных систем и данных с целью минимизировать возможность несанкционированного доступа.

Принуждение — метод защиты, предусматривающий соблюдение правил пользователями и персоналом работы с защищенными данными под угрозой административной или уголовной ответственности.

Побуждение — условия, побуждающие пользователей и персонал системы строго выполнять установленный порядок на основе соблюдения моральных и нравственных норм.

Защита информации осуществляется на различных направлениях: правовом, физическом, техническом, криптографическом.

Правовая защита информации — защита на основе законодательных нормативно-правовых актов, которые регулируют отношения субъектов по защите информации, а также наблюдение и контроль за их исполнением. В РФ к нормативно-правовым актам в области информационной безопасности относятся: Конституция РФ от 12.12.1993; Доктрина информационной безопасности РФ от 09.09.2000 № Пр-1895; ФЗ «Об информации, информационных технологиях по защите информации» от 27.0.2006 № 149; ФЗ «О персональных данных» от 27.07.2006 № 152.

«*Физическая* защита — защита информации на основе применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных субъектов к объекту защиты» [2]. В качестве таких средств могут быть использованы различные ограждения территории, помещений, окон, бронированные двери, сейфы для сохранности носителей информации. Сюда же можно отнести средства сигнализации и видеонаблюдения.

«Техническая защита — защита информации в соответствии с действующим законодательством с применением технических, программных и программно-технических средств» [2]. К техническим средствам защиты относятся механические, электрические, электронные, электронно-механические, оптические, лазерные, радиолокационные и т. д., которые встроены в информационные системы.

Программные средства — это средства защиты информации, которые работают в составе программного

обеспечения. Программные средства нацелены на внешнюю защиту — территория, здания, помещения, каналы связи, технические устройства автоматизированной системы. Программная поддержка реализации политики информационной безопасности обеспечивается (осуществляется) функциями и программными модулями, которые встроены непосредственно в программное обеспечение, создающее условия для хранения, обработки и передачи информации (операционные системы, системы управления базами данных, системы электронной почты, MRP/ERP-системы).

В настоящее время программные средства нашли применение в устройствах опознания личности: по голосу, отпечатку пальца, радужной оболочке глаза.

Криптографическая защита — защита информации на основе ее преобразования методами криптографии.

В зависимости от ценности информации, класса решаемых задач на предприятии определяется и степень защиты. Следовательно, для осуществления более надежного обеспечения защиты информации, особенно это касается крупных предприятий и корпораций, необходимо применять комплексную систему защиты, охватывающую комплекс правовых документов, организационных мер, программных, технических и криптографических средств.

К организационным средствам защиты информации относятся мероприятия, связанные с техническими и организационно-правовыми нормами, нацеленными (направленными) на обеспечение защиты данных в процессе создания (проектирование и разработка информационной системы, монтаж и наладка техники, проведение испытаний) и эксплуатации (создание пропускного режима, разработка интерфейса субъектов с автоматизированной системой, организация работы обслуживающего персонала и т. д.) средств вычислительной техники и автоматизированных систем. Для этого применяется метод ограничения доступа, заключающийся в создании

преграды по периметру объекта для защиты от доступа лиц, не наделенных специальными правами.

Цели защиты информации — исключить:

– незаконный доступ к информационным ресурсам и системам;

– возможность кражи, утраты, замены, модификации, подделки информации;

– несанкционированные действия по копированию, искажению, блокированию, удалению информации;

– возможность доступа субъекта к информации, содержащей конфиденциальные и персональные данные, находящиеся в информационных системах;

– возможность доступа к документированной информации как объекта собственности лиц, не наделенных правовыми полномочиями;

а также обеспечить:

– своевременное обнаружение источников угроз безопасности информации, ситуаций, которые наносят ущерб объекту;

– защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

Для достижения цели защиты информации необходим учет всех защищаемых ресурсов системы, осуществляемый, как правило, системным администратором; разделение полномочий доступа к информационным ресурсам и персональная ответственность каждого сотрудника, имеющего доступ к конфиденциальной информации и ресурсам информационной системы предприятия; использование программно-аппаратных средств защиты ресурсов системы, отслеживающих различные нарушения в обеспечении безопасности информации; периодическое проведение анализа эффективности использования применяемых средств и методов защиты информации предприятия.

В состав методов защиты информации входят методы ограничения и разграничения доступа.

Безопасность информации связана с защитой от угроз. Модель обеспечения защиты информации может быть представлена в следующем виде (см. рис. 4.5).

Рис. 4.5. Модель обеспечения защиты информации

4.3. Управление доступом. Идентификация и аутентификация

Понятие «управление доступом» подразумевает процесс обеспечения защиты информации при условии управления всеми ресурсами автоматизированной компьютерной системы. Это технические, программные, информационные средства.

Для обеспечения эффективной работы с информацией и вычислительной техникой, для достижения максимальной степени их защищенности, необходимо проведение разграничения доступа между пользователями системы.

Разграничение доступа пользователей к информации и средствам автоматизации осуществляется по таким параметрам, как:

– вид информации,
– степень ее секретности,
– назначение;
– выполняемые функции;
– способы и время обработки, и др.

В основу метода разграничения доступа заложен процесс идентификации. «Идентификация — присвоение объектам и субъектам доступа определенного идентификатора и (или) сравнение заявленного идентификатора с перечнем присвоенных идентификаторов». Иными словами, *идентификатор* — это признак, по которому определяется объект или субъект.

Цель идентификации — установление подлинности объекта или субъекта. Объектами идентификации могут быть человек, техническое устройство, носители информации, документы и т. д. В качестве идентификатора могут выступать коды паролей, которые содержатся в специальных носителях (электронные ключи, карточки), штрихкоды (например, произведенная продукция), биометрические системы опознания личностей (например, голос, отпечаток пальца, радужная оболочка глаза, ладонь).

Чаще всего при идентификации используются пароли, представляющие собой набор букв, символов, слов. Простые пароли проще запомнить, но их легче подобрать методом перебора или подсмотреть во время ввода в систему, поэтому они не обеспечивают надежную защиту. Для обеспечения более высокой степени защиты применяют более сложные пароли, которые трудно поддаются запоминанию и, поэтому записываются на специальные носители.

В паре с процессом идентификации выступает процесс аутентификации. «Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности» [14].

«Аутентификация или контроль подлинности (равенства, тождественности) состоит в проверке введенного (представленного) идентификатора пользователя или

устройства с целью получения допуска к системе или ее компонентам» [6].

Каждый объект или субъект заинтересован в обеспечении информационной безопасности. В связи с этим периодически проводится аудит паролей, используемых на объекте на подбор, взлом. Поэтому для обеспечения надежности парольной защиты необходимо управление сроками использования паролей, заменой, существенным повышением их сложности. Выполнение этих функций осуществляет, как правило, администратор.

В настоящее время, в век цифровых технологий, наблюдается замена многих бумажных документов субъектов на биометрическую идентификацию.

Для осуществления надежной защиты информации в настоящее время используется широкий спектр защитных мер, к которым относятся законодательные, морально-этические, организационные, физические, технические и программные средства. Комплексное использование этих средств обеспечивает более высокую степень защиты. При этом необходимо заметить, что разработка комплекса мер по защите информации должна осуществляться параллельно с процессом проектирования и создания информационной системы. Только в этом случае можно проработать все требования к обеспечению безопасности системы на основе изучения ее узких мест и надежно защитить такую систему. Система защиты информации не может быть создана однажды и навсегда; это мероприятие не одномоментно, а непрерывный процесс принятия надлежащих мер на всех стадиях жизненного цикла системы, начиная со стадии проектирования до стадий внедрения и эксплуатации. Не существует совершенной, непреодолимой системы защиты. Любую систему защиты можно взломать, вопрос упирается лишь в количество времени и используемых средств и в квалификацию специалиста в этой области. Создание высокоэффективной системы защиты информации — дорогостоящий процесс. Поэтому необходимо соблюдать баланс

между ценностью защищаемой информации, систем, технологий и затратами, связанными с обеспечением безопасности, т. е. уровень защиты должен быть достаточным, чтобы риск, затраты и возможность причиненного убытка были бы приемлемы. Не последняя роль отводится и персональной ответственности каждого сотрудника, наделенного определенными полномочиями и обязанностями [6].

4.4. Криптография и стеганография

На Руси криптография впервые появилась при царе Иване IV. Дальнейшее ее развитие продолжалось во время правления Екатерины II. С приходом к власти Александра I (начало XIX века) криптографическое преобразование информации было отдано в делопроизводство Канцелярии Министерства иностранных дел Российской империи.

В настоящее время криптография стала неотъемлемой частью общества, которая используется в электронном документообороте, электронной коммерции, в сотовой связи, цифровом телевидении, банковских операциях и т. д. Криптография рассматривается как отдельное научное направление, опирающееся на тесную взаимосвязь математики и информатики.

Понятие «криптография» подразумевает преобразование исходной информации с помощью математических законов, позволяющих обеспечить ее защиту от лиц, не наделенных специальными полномочиями. Особенно это касается конфиденциальной информации при передаче ее по каналам связи. Применение криптографических методов (см. рис. 4.6) обеспечивает контроль целостности программного обеспечения по контрольным суммам, электронной подписи финансовых документов. При кодировании и декодировании информации (обратном преобразовании) могут быть сиспользованы специальные словари, таблицы. Прочесть зашифрованную информацию возможно только при знании ключа. Таким образом,

шифрование — это преобразование исходного (открытого) текста в зашифрованный с использованием ключа. Ключом может служить информация в виде набора слов, букв, символов, цифр, который используется как для шифрования, так и обратного действия — расшифрования (дешифрования).

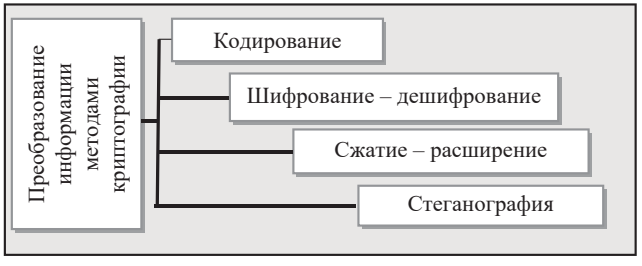


Рис. 4.6. Криптографические методы преобразования информации

Методы шифрования включают два класса: с симметричным ключом и с несимметричным (отрытым) ключом (см. рис. 4.7). Симметричность заключается в использовании обеих сторон одного и того же ключа. Шифрование и дешифрование производится одним ключом. Поэтому этот ключ является секретным. Достоинство симметричных методов заключается в их высокой криптостойкости и достаточной изученности, поэтому они могут использоваться для уверенной аутентификации сообщений.

К способам шифрования с симметричным ключом относится *метод замены* (подстановки), который заключается в замене букв исходной информации, принадлежащих одному алфавиту на буквы другого алфавита.

Рассмотрим другой метод подстановки (замены), основанный на использовании таблицы Вижинера. В основу данного метода лежит квадратная матрица с m^2 элементами, где m — число букв используемого алфавита.

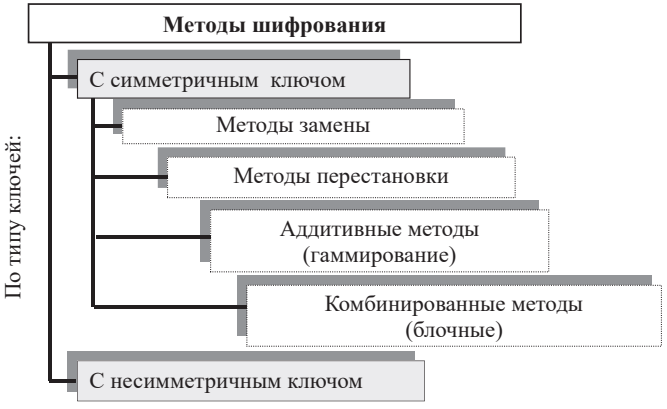


Рис. 4.7. Классификация методов шифрования

Первая строка матрицы содержит последовательность букв алфавита. Вторая и последующие строки заполняются буквами со сдвигом на одну, две, три и т. д. позиции, освободившиеся места заполняются недостающими буквами (см. рис. 4.8). Размер представленной в примере матрицы 31x31 (русский алфавит, с исключением букв «Ё» и «Й»).

А	Б	В	Г	Д	Е	...	...	...	...	...	...	Э	Ю	Я
Б	В	Г	Д	Е	Ж	...	...	...	...	...	...	Ю	Я	А
В	Г	Д	Е	Ж	З	...	...	...	...	...	...	Я	А	Б
Г	Д	Е	Ж	З	И	...	...	...	...	...	...	А	Б	В
Д	Е	Ж	З	И	К	...	...	...	...	...	...	Б	В	Г
Е	Ж	З	И	К	Л	...	...	...	...	...	...	В	Г	Д
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
Я	А	Б	В	Г	Д	...	...	...	...	...	...	Ь	Э	Ю

Рис. 4.8. Исходная матрица-алфавит для метода Вижинера

Шифрование текста будем осуществлять с использованием ключа, представляющего собой слово, в котором не должна повторяться ни одна буква, например, *солнце*, *компьютер*, *сирена* и т. п. В нашем случае в качестве ключа будет использоваться слово «***комар***».

Текст, который будем шифровать методом Вижинера:

Ц	И	Ф	Р	О	В	А	Я		Э	К	О	Н	О	М	И	К	А

Технология кодирования текста методом Вижинера показана на рис. 4.9. Согласно этой технологии, первая буква исходного текста (буква Ц) отыскивается в основной строке алфавита, а соответствующий ей знак находим в первой строке ключевого слова в столбце под этой буквой (буква Я). Вторая буква исходного текста (буква И) берется также в строке алфавита, и на пересечении со второй строкой ключевого слова и столбца находится соответствующий ей знак (буква Ц) и т. д.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л
А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П

Рис. 4.9. Технология кодирования методом Вижинера

Полученный зашифрованный текст (методом Вижинера):

Я	Ц	Я	Р	Э	М	О	Л		Э	Щ	Ч	Ъ	Щ	М	Ш	У	О

Рис. 4.10. Технология кодирования методом Вижинера

Процессы шифрования и дешифрования реализуются по одному и тому же принципу. Надежность данного метода зависит от длины ключа, тем не менее, очень длинные ключи создают определенные трудности.

Метод перестановки — метод малой сложности преобразования сообщений, который имеет смысл использовать в сочетании с другими методами. Примером метода перестановки является метод Гамильтона, предстающий в виде восьмиэлементной схемы маршрутов — таблица 1 (см. рис. 4.11).

В данном примере необходимо зашифровать исходное сообщение: КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ. При этом ключ равен: 1, 2, 2, 1. Для шифрования будем использовать исходную таблицу и два маршрута.

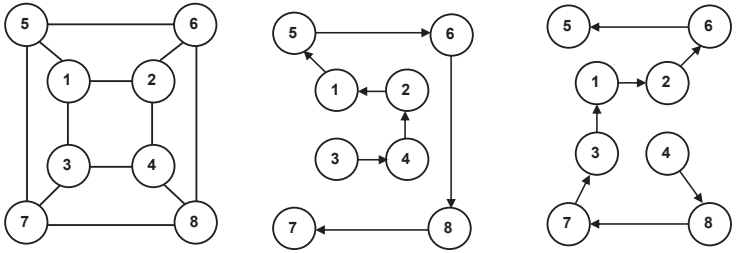


Таблица 1Маршрут 1 Маршрут 2

Рисунок 4.11. Элементная таблица и маршруты Гамильтона

Ход шифрования по методу Гамильтона следующий:

1. Исходное сообщение разбиваем на четыре блока (по 8 символов):

1) **КРИПТОГР** 2) **АФИЧЕСКО** 3) **Е_ПРЕОБР** 4) **АЗОВАНИЕ**

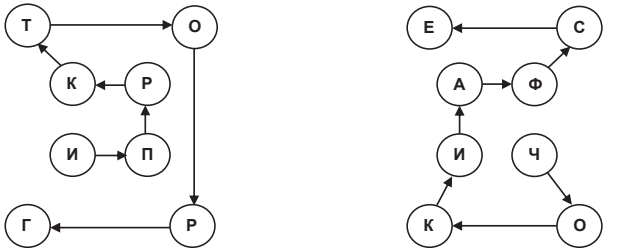
Примечание. Если в таблице маршрута остаются свободные кружки из-за оконченного текста, то в таком случае они заполняются знаком *.

Размещаем буквы исходного текста в маршрутах Гамильтона (см. рис. 4.12).

2. Получение шифртекста путем записи букв в соответствии с маршрутами (по ключу: 1, 2, 2, 1):

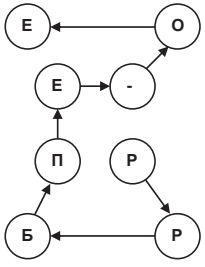
ИПРКТОРГЧОКИАФСЕРРБПЕ_ОЕОВЗААНЕИ

Аддитивные методы (гаммирование) — при данном методе исходный текст подлежит наложению на некоторый хаотичный набор случайных чисел. Суть методов — последовательное суммирование цифровых кодов, которые соответствуют символам исходного текста, с последовательностью кодов, которая соответствует кортежу символов, называемых гаммой.

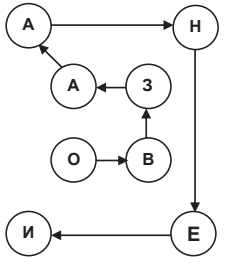


Маршрут 1

Маршрут 2



Маршрут 2



Маршрут 1

Рис. 4.12. Пример шифрования с помощью маршрутов Гамильтона

*Комбинированные (*блочные*) методы* — последовательность методов преобразования применительно к части (блоку) исходного текста. Размер блоков может меняться в пределах 64—256 бит [9].

Симметричное шифрование может применяться пользователями, обменивающимися своими сообщениями и находящимися на значительном расстоянии друг от друга. Зашифрованные сообщения могут быть записаны на сменные носители с тем, чтобы никто из посторонних лиц не мог их прочитать.

Примером простой подстановки является метод Цезаря.

Шифр Цезаря, согласно материалу из Википедии (свободной энциклопедии), иначе называется **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря,** как частный случай кодирования методом шифра простой замены (иначе может называться одноалфавитной подстановкой), представляет собой один из самых несложных и признанных методов шифрования. Этот метод позаимствовал свое название от имени римского императора Гая Юлия Цезаря. Цезарь применил такой метод шифрования для переписки с Цицероном (примерно 50 г. до н. э.).

Подробно метод шифрования Цезаря рассмотрен во множестве источников (см. [15]).

Рассмотрим работу данного метода кодирования на примере Microsoft Excel.

1-й шаг. На листе «Шифровать» исходный текст разбивается на отдельные символы в обратном порядке.

=ЕСЛИ(B3<=$A$2;**ПСТР**($A$1;$A$2-B3+1;**1**);" ")

Здесь в ячейке A1 расположен исходный текст, в ячейке A2 расположена рассчитанная длина исходного текста (=ДЛСТР(A1)), в ячейке B3 расположен номер текущего символа в исходном тексте (=ЕСЛИ(ИЛИ(B3+1>$A $2;B3=0);0;B3+1)), ячейка B2 пустая, ячейка B3 содержит число 1, ячейка B4 (и большие по номеру) содержит номер на 1 больше предыдущего.

2-й шаг. Каждому символу противопоставляется его цифровой код в кодировке ASCII.

=**КОДСИМВ**(A3)

3-й шаг. Цифровой код увеличивается (или уменьшается) на заранее определенное число (здесь ключ равен 3).

=КОДСИМВ(A3)+**3**

4-й шаг. Полученное новое цифровое значение преобразуется в соответствующее символьное значение, согласно таблице ASCII.

=ЕСЛИ(A3=" ";"";**СИМВОЛ**(КОДСИМВ(A3)+3))

5-й шаг. Полученные символы объединяются в новый (закодированный) текст в обратном порядке.

=**СЦЕПИТЬ**(C12;C11;C10;C9;C8;C7;C6;C5;C4;C3)

Здесь использовано ограничение: 10 символов исходного текста.

Рассмотрим работу метода Цезаря по раскодированию на примере Microsoft Excel.

1-й шаг. На листе «Расшифровать» кодированный текст разбивается на отдельные символы в обратном порядке.

=ЕСЛИ(B3<=$A$2;**ПСТР**($A$1;$A$2-B3+1;**1**);" ")

Здесь в ячейке A1 расположен кодированный текст, в ячейке A2 расположена рассчитанная длина кодированного текста (=ДЛСТР(A1)), в ячейке B3 расположен номер текущего символа в кодированном тексте =ЕСЛИ(ИЛИ(B3+1>$A$2;B3=0);0;B3+1)), ячейка B2 пустая, ячейка B3 содержит число 1, ячейка B4 (и большие по номеру) содержит номер на 1 больше предыдущего.

2-й шаг. Каждому символу противопоставляется его цифровой код в кодировке ASCII.

=**КОДСИМВ**(A3)

3-й. шаг. Цифровой код уменьшается (или увеличивается) на заранее определенное число (здесь ключ равен 3).

=КОДСИМВ(A3)-**3**

4-й шаг. Полученное новое цифровое значение преобразуется в соответствующее символьное значение, согласно таблице ASCII.

=ЕСЛИ(ИЛИ(A3=" ";A3="");"";**СИМВОЛ**(КОДСИМВ(A3)-3))

5-й шаг. Полученные символы объединяются в новый (раскодированный) текст в обратном порядке.

=**СЦЕПИТЬ**(C12;C11;C10;C9;C8;C7;C6;C5;C4;C3)

Здесь использовано ограничение: 10 символов кодированного текста.

В настоящее время существует много разновидностей кодирования на основе метода Цезаря. Например, аффинная система метода подстановок Цезаря, основанная на операции одновременного сложения и умножения по модулю; система шифрования методом Цезаря с использованием ключевого слова, основанная на применении небольшого ключевого слова (меньше длины сообщения) для смещения и пересортировки символов в заранее установленном алфавите подстановки. Для

повышения степени защиты могут использоваться сразу несколько методов кодирования.

Развитие криптографии не стоит на месте, наметились новые направления. Это квантовые вычисления и квантовая криптография, требующие использования более совершенной техники — квантовых компьютеров, но это вопрос будущего.

Одновременно с шифрованием текста часто применяют:

– электронная цифровая подпись;
– контроль доступа к данным;
– обеспечение целостности данных и др.

«Электронная цифровая подпись (ЭЦП) — средство защиты целостности и подтверждения авторства электронного документа, которое функционирует на основе определенных криптографических методов» [14].

Современные информационные системы используют пару ключей для шифрования: открытый ключ (*public key*), доступный любому пользователю, и закрытый ключ (*private key*), доступный ограниченному числу пользователей. Пара таких ключей применяется для шифрования текста, а также для генерации ЭЦП и дальнейшей проверки ее целостности. При этом:

– зашифрованное на основе открытого ключа информационное сообщение будет расшифровано только при использовании соответствующего (парного ему) закрытого ключа.

– ЭЦП, сгенерированная на основе закрытого ключа, может быть проверена на целостность только при использовании соответствующего (парного ему) открытого ключа.

Для действия ЭЦП генерируется секретный ключ (СК). В создании ЭЦП участвует СК, который накладывается на значение хэша электронного документа, рассчитанного на основе определенной хэш-функции. Хэш (аналог контрольной суммы) является рассчитанным автоматически значением, полученным на основе содержимого электронного документа. Внесение любого изме-

нения в документ влечет автоматическое изменение его хэша. Использование современных алгоритмов ЭЦП, например, ГОСТ Р 34.10—94 и ГОСТ Р 34.11—94, полностью исключают возможность подделать хэш электронного документа.

В некоторых случаях СК шифруют с паролем. При этом значение открытого ключа (ОК) формируется на основе значения определенной функции из СК, что затем применяется для проверки ЭЦП. ОК передается по любому открытому каналу связи (флэшка, локальная сеть). В момент проверки ЭЦП на ее основе рассчитывается значение хэша электронного документа. Обнаружение различия вычисленной ЭЦП с переданной является сигналом нарушения его подлинности (целостности).

ЭЦП может устанавливаться:

– для любого элемента информационного сообщения,
– для идентификатора пользователя,
– открытого ключа пользователя,
– срока действительности ключа пользователя.

«При создании (генерации) ЭЦП на доверителя возлагается важная функция по проверке подлинности закрепленных за ним открытых ключей. Доверителями могут быть: отдельные пользователи, удостоверяющие центры» [6]. Такие центры выступают ключевым звеном в цепочке проверки подлинности открытых ключей для ЭЦП (см. рис. 4.13).

«Распределение открытых ключей может выполняться с помощью квалифицированных сертификатов ключей проверки ЭЦП» [6]. Эти квалифицированные сертификаты являются электронными документами (контейнерами), включающими в себя как открытый ключ пользователя, так и непосредственно данные, подтверждающие принадлежность и правила применения этого ключа. В этом случае повышается надежность при подтверждении подлинности включенных в квалифицированные сертификаты открытых ключей, а также однозначная идентификация их владельцев.

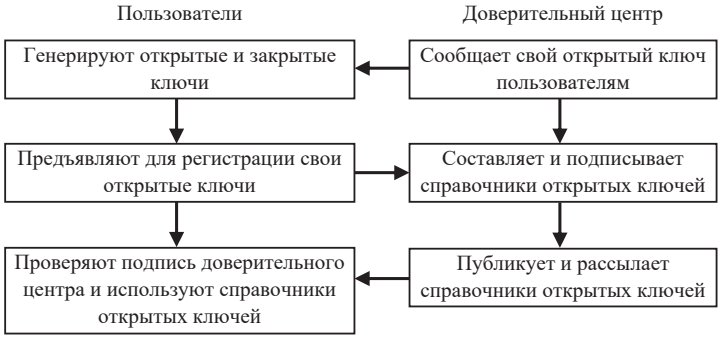


Рис. 4.13. Схема передачи открытых ключей удостоверяющим центром

Вызывает интерес скрытная передача небольших данных. Эту функцию полностью покрывает стеганография.

Стеганография (τεγανός — скрытый + γράφω — пишу) — дословно «скрытопись», согласно материалу из Википедии (свободной энциклопедии), составляет искусство передавать важные (в данном случае сокрытые) данные, в составе (т. е. внутри) других (в данном случае открытых) данных по обычным (в данном случае открытым) каналам связи (например, электронная почта, флэшка). Скрываемые данные являются стегосообщением, а данные, содержащие внутри себя стегосообщение, выступают контейнером (в данном случае стегоконтейнером).

В настоящее время разработано и существует огромное множество алгоритмов информационной стеганографии. Это и DarkJPEG, «TCP стеганография», ну и, конечно, особое место занимает любимый всеми студентами «алгоритм LSB» (например, LSB стеганография, стеганография в файлах GIF).

При создании файлов формата **jpg** (изображение) и **ppm** срабатывает механизм сжатия, что само по себе создает вероятность сокрытия важной информации в таких файлах (например, в случае действия алгоритма «сжатия без потерь»). Процесс включения важной

информации в выбранное изображение (донор или контейнер), например, выполняется LSB-методом. Срабатывает механизм смешивания цветов RGB (Red-красный, Green-зеленый, Blue-голубой) и каждая точка (пиксель рисунка) кодируется тремя байтами. Согласно данному механизму, изменения каждого из трех бит (выбираются наименее значимые) точки-пикселя может изменить менее 1% интенсивности (яркости) всего изображения, что не обнаруживается визуально (обычным взглядом). В таком случае в файле JPG (или BMP) объемом 1600 килобайт спокойно «вмонтируется» примерно 200 килобайт важных данных. Вместе с тем, при автоматическом задействовании Звышеописанного алгоритма возникает элемент случайности. Он может повлиять на параметры изображения, что возможно определить по фрагменту однотонной (один цвет) заливки средствами статистического анализа.

Исследуем возможности данного статистического анализа на примере произвольной скрин-картинки (здесь на рис. 4.14 фотография Н. Кейджа):

Рис. 4.14. Николас Кейдж (актер)

С помощью алгоритмов, основанных на визуальной атаке, преобразуем исходную скрин-картинку в новую, составив ее из значащих бит по определенным цветовым разрядам (см. рис. 4.15).

Обращают на себя внимание второе и третье изображения, где присутствуют «помехи» в виде областей

с высокой энтропией, что вызвано высокой плотностью данных в рассматриваемом изображении. С наибольшей долей вероятности в данном изображении содержится внедренное (скрытое) сообщение.

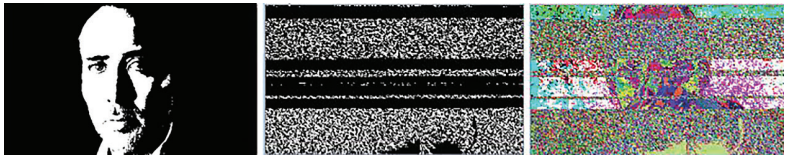


Рис. 4.15. Преобразование картинки

Но такой визуальный анализ почти невозможно автоматизировать системно.

На текущий момент известно несколько приемов (методов) по нахождению внедренных сообщений в виде заполненных контейнеров. Основу этих действий составляют статистические параметры изображения в виде утверждения, что заполненный контейнер повышает энтропию. Это утверждение подтверждается тем, что из-за ограничения емкости занимаемого сообщением контейнера такое сообщение, скорее всего, будет сжато и/или зашифровано (т. е. происходит уплотнение данных). Все это естественно увеличивает энтропию изображения.

В последнее время возможности стеганографии становятся темой научных дискуссий. Так, есть предположение, что террористы применяли стеганографию при организации терактов 11 сентября 2001 года. Вместе с тем, прямых доказательств пока этому нет. Все это подогревает интерес к использованию стеганографии в качестве эффективного средства сокрытия важной информации.

Применение средств стеганографии отмечено в некоторых вредоносных программах и средствах ведения кибершпионажа, например:

- Microcin (*AKA six little monkeys*);
- NetTraveler;
- Zberp;

- Enfal (*its new loader called Zero.T*);
- Shamoon;
- KinS;
- ZeusVM;
- Triton (*Fibbit*).

Можно поставить вопрос: почему авторы вредоносного программного обеспечения так активно применяют средства стеганографии в своих разработках? Здесь следует отметить следующие основные причины использования методов стеганографии:

- позволяют скрыть как сами данные, так и присутствие факта процесса их загрузки/выгрузки;
- дает возможность обойти DPI-системы, что бывает необходимо в корпоративных информационных сетях;
- позволяет обойти проверку в AntiAPT-продуктах, т. к. эти продукты зачастую не способны обрабатывать все графические файлы из-за их огромного количества, а алгоритмы для выполнения такого анализа имеют высокую стоимость.

Таким образом, следует сделать вывод:

- применение возможностей стеганографии сегодня очень популярно среди разработчиков вредоносного и шпионского программного обеспечения;
- возможности антивирусных программ и средств защиты периметра корпоративных сетей демонстрирцуют низкую эффективность при проверке заполненных контейнеров, т. к. их очень трудно обнаружить;
- имеющиеся на настоящий момент программы по обнаружению следов стеганографии относятся к PoC (*Proof-of-Concept*), т. е. их алгоритм невозможно внедрить в промышленные средства защиты информации по причине низкой скорости работы, а также недостаточно надежного уровня обнаружения.

4.5. Компьютерные вирусы антивирусная защита. Ответственность за компьютерные преступления

Компьютерный вирус является программой, специально созданной для автоматического прикрепления к любым другим программам, а также для самостоятельного создания копии самого себя и автоматического внедрения в некоторые файлы, основные системные области как одного компьютера, так и других компьютеров, объединенных с ним в локальную сеть [14]. Компьютерный вирус предназначен для нарушения работы других программ, порчи содержимого файлов и директорий, в том числе создания других помех при работе на компьютерах.

Признаков появление вирусов (заражения) в компьютере может быть несколько (см. рис. 4.16).

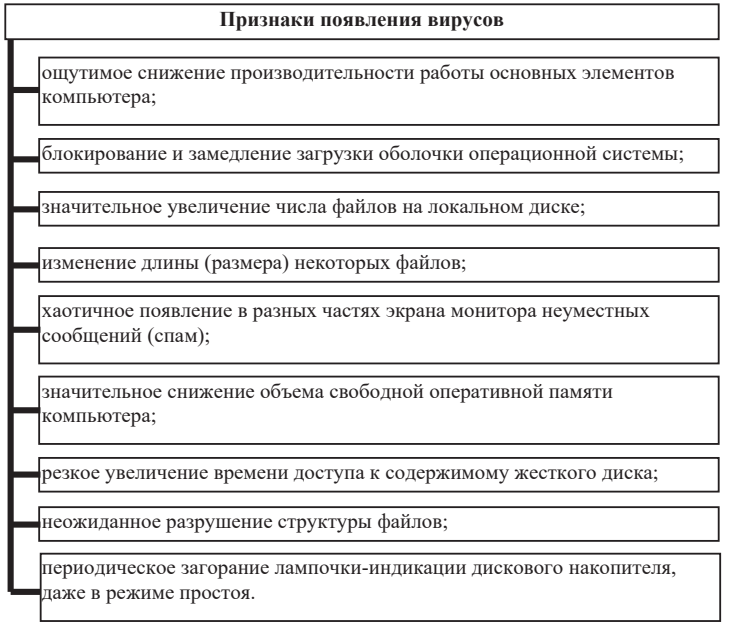


Рис. 4.16. Признаки появления вирусов

Одними из основных способов заражения вирусами обычно служат съемные диски (флэшки и CD-ROM) и атака из компьютерных сетей. Момент заражения основных устройств компьютера происходит при установке и открытии содержимого съемного (завирусованного) диска.

Вирусы различают по среде обитания: загрузочныме, файловые, системные, сетевые и файлово–загрузочные (см. рис. 4.17).

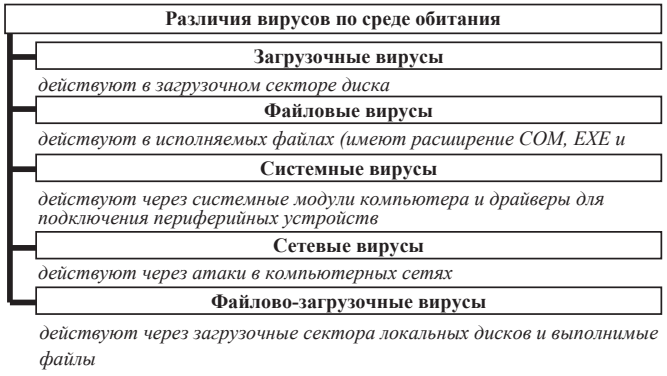


Рис. 4.17. Различия вирусов по среде обитания

По пути заражения среды обитания вирусы разделяют на резидентные и нерезидентные (см. рис. 4.18).

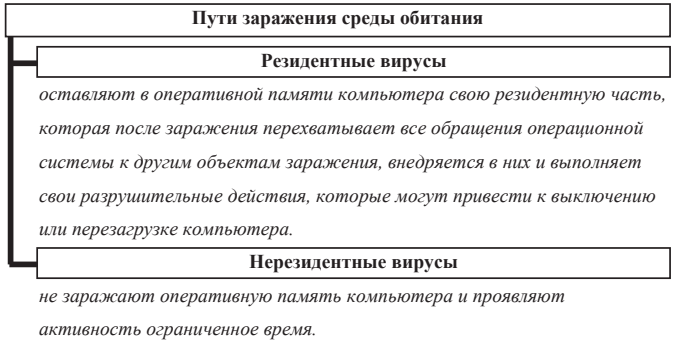


Рис. 4.18. Различия вирусов по пути заражения среды обитания

Особенность построения вирусов влияет на их проявление и функционирование (см. рис. 4.19).

Анализируя степень воздействия на компьютерные ресурсы, выделяют безвредные, неопасные, опасные и разрушительные вирусы (см. рис. 4.20).

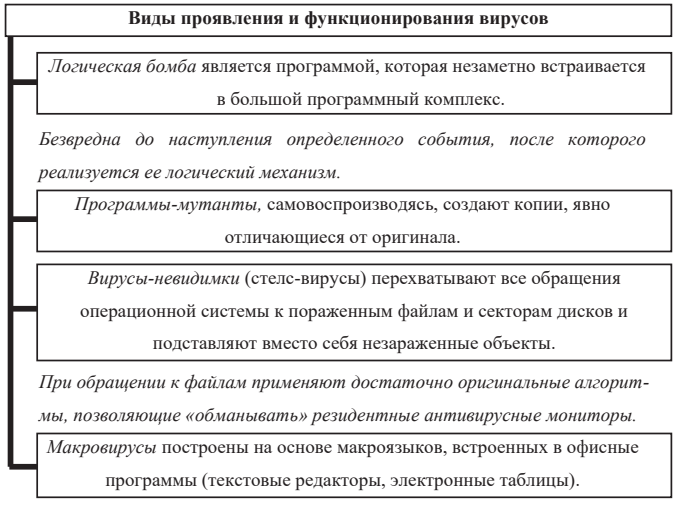


Рис. 4.19. Виды проявления и функционирования вирусов

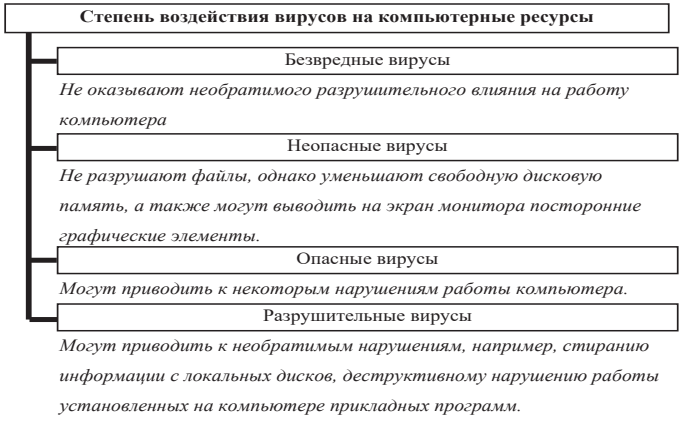


Рис. 4.20. Степень воздействия вирусов на компьютерные ресурсы

Следует помнить, что любой выполнимый или автозагружаемый файл может содержать вирус.

Антивирусные программы

Для противодействия компьютерным вирусам создано большое число антивирусных программ, обнаруживающих и ликвидирующих вирусы в разных операционных системах.

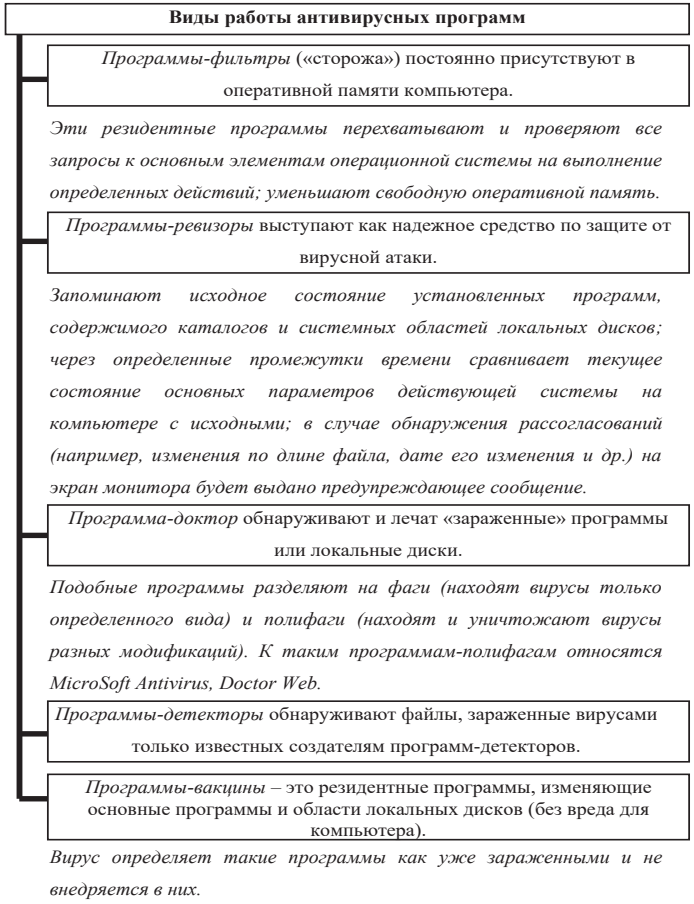


Рис. 4.21. Виды работы антивирусных программ

В основе работы антивирусных программ лежит обнаружение сигнатуры вирусов (т. е. кода тела вируса).

Виды работы антивирусных программ: фильтры, ревизоры, доктора, детекторы, вакцины и др. (см. рис. 4.21).

Ответственность за компьютерные преступления

Мероприятия по защите важной информации строятся в соответствии с нормативной базой документов (см. рис. 4.22).

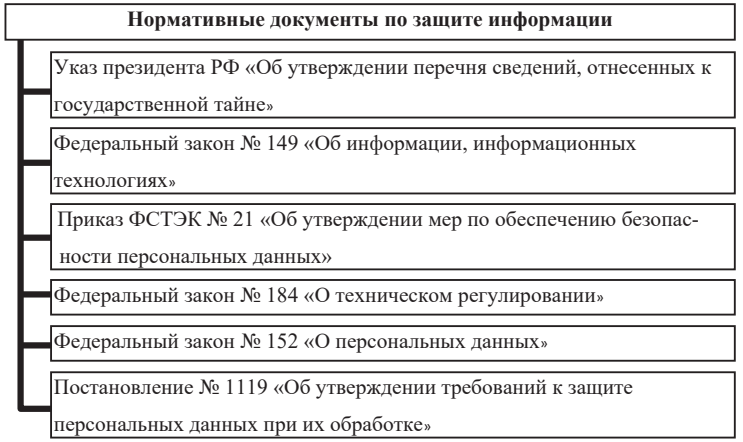


Рис. 4.22. Основные документы по защите информации

Согласно этим документам, компьютерным правонарушением (преступлением) (*computercrime*) обозначают противоправные действия, выполненные с применением средств вычислительной техники. Предметом и (или) средством совершения такого правонарушения являются средства вычислительной техники и компьютерные данные (информация).

В соответствии с «Конвенцией о киберпреступности», принятой на заседании Совета Европы, можно выделить

четыре группы правонарушений (преступлений) (см. рис. 4.23).

В текущем российском уголовном законодательстве четко прописан состав преступлений, относящихся к компьютерным данным (информации) (см. рис. 4.24, 4.25, 4.26).

Основные группы правонарушений (преступлений)

- Правонарушения (преступления), направленные против конфиденциальности, а также целостности и доступности компьютерных данных (информации) и компьютерных систем

  незаконный доступ, перехват, воздействие на сами данные, воздействие на надежность функционирования системы, незаконное использование дополнительных устройств

- Правонарушения (преступления), направленные на использование компьютерных средств

  мошенничество с применением компьютерных технологий

- Правонарушения (преступления), направленные на искажение данных
- Правонарушения (преступления), направленные на авторские права и смежные права

Рис. 4.23. Основные группы правонарушений (преступлений) по «Конвенции о киберпреступности»

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации»

состав преступления имеет материальный характер и влечет последствия

- за уничтожение компьютерных данных (информации);

стирание данных в памяти компьютера с невозможностью восстановления

- блокирование компьютерных данных (информации);

специально созданное затруднение доступа к компьютерным данным (информации), вместе с тем не связанное с ее уничтожением

- модификация компьютерных данных (информации);

внесение в данные любых изменений

- копирование компьютерных данных (информации);

повторение и устойчивое запечатление ее на машинном или ином обособленном носителе

- нарушение работы компьютеров, компьютерной сети;

временное или устойчивое создание помех для их функционирования в соответствии с назначением

- неправомерный доступ к компьютерным данным (информации) для лиц, не имеющих права на доступ к этим данным; для лиц, имеющих такое право, но выполняющих его вне регламентированного порядка, с нарушением правил защиты данных.

наказание

до 2 лет лишения свободы, а при отягчающих обстоятельствах – до 5 лет

субъект правонарушения (преступления)

вменяемое физическое лицо, достигшее 16 лет

Рис. 4.24. Особенности статьи 272 УК РФ

Статья 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»
состав преступления
- за создание программ для компьютеров или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, к нарушению работы компьютеров, компьютерной сети;
- за использование либо распространение программ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, к нарушению работы компьютеров, компьютерной сети, или машинных носителей с такими программами.
наказание
до 3 лет лишения свободы, а при отягчающих обстоятельствах – до 7 лет
субъект правонарушения (преступления)
вменяемое физическое лицо, достигшее 16 лет

Рис. 4.25. Особенности статьи 273 УК РФ

Статья 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»
состав преступления
- за нарушения правил эксплуатации компьютеров, компьютерной сети, повлекшие уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.
наказание
до 2 лет лишения свободы, а при отягчающих обстоятельствах – до 4 лет
субъект правонарушения (преступления)
вменяемое физическое лицо, достигшее 16 лет

Рис. 4.26. Особенности статьи 274 УК РФ

Вопросы для самоконтроля

1. Дайте определение информации.
2. Назовите и охарактеризуйте предмет и объект защиты информации.

3. Назовите и охарактеризуйте основные свойства информации.
4. Дайте определение ценности информации.
5. Охарактеризуйте коммерческую и государственную тайну информации.
6. Назовите и охарактеризуйте основные угрозы безопасности информации.
7. Назовите и охарактеризуйте основные этапы развития криптографии.
8. Дайте определение криптологии, криптографии и криптоанализа.
9. Сформулируйте основные направления в современной криптографии.
10. Дайте определение основных понятий криптографической защиты информации.
11. Сформулируйте основные требования к криптосистемам.
12. Приведите классификацию методов криптографического преобразования информации.
13. Каковы перспективы криптозащиты информации в КС.
14. Дайте определение электронной цифровой подписи.
15. Охарактеризуйте основной принцип использования открытого и закрытого ключа для электронной цифровой подписи.
16. Охарактеризуйте основные принципы работы управляющего центра при передаче открытых ключей.
17. Дайте определение стеганографии.
18. Охарактеризуйте основной принцип работы компьютерной стеганографии методом LSB.
19. Охарактеризуйте способ нахождения внедренного сообщения в файл-изображение.
20. Назовите и охарактеризуйте причины использования стеганографии авторами вредоносного программного обеспечения.

21. Назовите и охарактеризуйте основные методы защиты информации.

22. Назовите и охарактеризуйте основные направления защиты информации.

23. Назовите и охарактеризуйте основные цели защиты информации.

24. Охарактеризуйте модель обеспечения защиты информации.

25. Назовите и охарактеризуйте основные признаки появления вирусов.

26. Назовите и охарактеризуйте типы вирусов по среде обитания.

27. Перечислите основные нормативные документы в сфере защиты информации.

28. Дайте определение компьютерного преступления.

29. Назовите и охарактеризуйте четыре группы преступлений, согласно «Конвенции о киберпреступности».

30. Назовите и охарактеризуйте основные статьи уголовного законодательства в области компьютерных преступлений.

31. Дайте определение управления доступом к информации.

32. Дайте определение идентификации.

33. Дайте определение аутентификации.

Список использованных источников главы 4

1. ГОСТ Р 34.10—2001. ИТ. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Изд-во Стандартов, 2013.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст. 3448.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», ст. 4736.

4. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 09 сентября 2000г. — М.: «Информациология, 2000.

5. Информационная безопасность: Учебник / В. П. Мельников, А. И. Куприянов. — М.: Кнорус, 2018.

6. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации: Учебное пособие. — М.: Ленанд, 2019.

7. Борисов М. А., Романов О. А. Особенности организационно-правовой защиты информации. — М.: Ленанд, 2018.

8. Борисов М. А. Особенности защиты персональных данных в трудовых отношениях. — М.: Ленанд, 2017.

9. Мельников В. П., Схиртладзе А. Г. Методы и средства хранения и защиты компьютерной информации. — Старый Оскол: ТНТ, 2014.

10. Нестеров С. А. Основы информационной безопасности: Учеб. пособие. — СПб.: Изд-во Политехн. ун-та, 2014.

11. Официальный сайт ФСТЭК России. — URL: http://www.fstec.ru

12. Официальный сайт Федерального агентства по техническому регулированию и метрологии ((Росстандарта). — URL: http://standard.gost.ru

13. Национальный стандарт РФ. ГОСТ Р 50922—2006. «Защита информации. Основные термины и определения», утвержден Пр. Росстандарта РФ от 27.12.2006 №373-ст.;

14. Руководящий документ ФСТЭК РФ, «Защита от несанкционированного доступа к информации», утвержденного Решением Председателя Гостехкомиссии РФ от 30.03.1992

15. Циммерманн Ф. Введение в криптографию. — PGP Corporation, 2004

5.1. Стартапы. Характеристики, компоненты, отличительные особенности

Стартап — вновь созданная организация, временная структура, компания с короткой операционной историей, которая занимается разработкой новых товаров или услуг, поиском воспроизводимой, прибыльной, рентабельной и масштабируемой бизнес-модели, развитием или исследованием перспективных рынков в условиях чрезвычайной неопределенности. Также важно понимать, что стартапы зачастую используют достижения технического прогресса, а не двигают его вперед. Стартап может не являться юридическим лицом, создается под воплощение в жизнь конкретной идеи, финансирование в большей степени осуществляется за счет внешних инвесторов.

К характерным признакам стартапа, отличающим его от недавно созданных и малых предприятий, относятся...

Стартап представляет собой несколько расплывчатое понятие. Так что стоит рассмотреть присущие ему свойства, которые признаны большинством предпринимателей.

Таблица 5.1

Основные свойства стартапов

Ориентированность на инновации	Нередко смысл стартапов заключается в продвижении инноваций либо модернизации прежних идей. За счет этого они способны тягаться с крупными корпорациями, чаще всего не задумывающимися о внедрении новаторских идей и продолжающими реализовывать услуги и продукцию с уже устоявшейся коммерческой репутацией. По этой причине стартап — затея всегда рискованная, своего рода шаг в неизвестность.
Уникальная идея	Нет идеи — нет бизнеса. Но в стартапе она имеет первостепенное значение. Перспективная идея может быть весьма дорогостоящей. Допустим, во Всемирной паутине представлена масса шаблонных идей для открытия своего дела, и они не стоят ни копейки. Порой они сопровождаются готовыми бизнес-планами https://startupnetwork.kz/sale/
Стартапы создает молодежь	Возраст большинства удачливых стартаперов не превышает 25 лет. Поэтому многие пренебрежительно называют стартапы «гаражным бизнесом»: вчерашние выпускники вузов, не имеющие ни гроша за душой, вынуждены собираться в арендованных помещениях и гаражах, чтобы поделиться своими идеями.
Пан или пропал	Стартаперы обычно прилагают максимум усилий для претворения своей идеи в жизнь, не боясь поставить на карту все. Их не особенно беспокоит то, что победа может стоить чересчур дорого: если они по-настоящему хотят этого, то сделают все, чтобы осуществить свою мечту.
Работа за идею	Развивать дело самостоятельно очень трудно, вследствие этого в создании стартапа принимает участие команда энтузиастов с лидером во главе. Один может быть занят разработкой идеи, другой — написанием бизнес-плана на ее основе, третий — поиском клиентов, поставщиков, вкладчиков. Причем, трудятся они именно за идею, а не ради денег, по крайней мере, на начальном этапе.
Денежные трудности	Нехватка финансовых ресурсов для воплощения идеи в жизнь является основной характерной чертой стартапов. Это и понятно, поскольку их создают молодые люди, у которых полно энергии, но нет средств. Вот почему стартапам необходима помощь инвесторов. Разумеется, вкладчиков не может не соблазнять прибыль.

Окончание таблицы

Таблица 5.2

Преимущества и недостатки стартапов

Преимущества	Недостатки
• Высокая доходность	• Высокие риски
• Мобильность	• Малые «размеры»
• Статус монополиста, отсутствие прямых конкурентов	• Проблемы финансирования

Основные стадии (этапам развития) стартапа

1. Посевной этап, или Pre-Seed stage. На данном этапе происходит поиск идеи и разработка технических способов ее реализации. Инициативная группа проводит анализ рынка, пишет бизнес-план, формулирует техзадание. Далее следуют: создание прототипа продукта, тестирование его версий, изучение спроса и поиск источников финансирования. Если не удается найти инвестора, проект «затухает». Увы, с большинством стартапов именно это и случается.

2. Запуск, или Startup Stage. Итак, инвестор найден: продукт можно выпускать на рынок. Оказавшись в рыночных условиях, продукт должен доказать свое преимущество перед аналогами. Но на этом этапе обойти конкурентов не так-то просто. Создателям стартапа следует проявить упорство, продемонстрировать творческое мышление и деловую хватку. Именно сейчас проект подвергается наибольшему риску. Если целевая аудитория останется равнодушной, его история на том и завершится.

3. Рост, или Growth Stage. Допустим, проект выжил в конкурентной борьбе. Продукт пользуется спросом и потихоньку захватывает рыночную нишу, на которую ориентировались его разработчики. Настаёт время выходить на точку безубыточности и приносить инвесторам кое-какую прибыль.

4. Расширение, или Expansion Stage. Цели, отраженные в бизнес-плане, наконец-то достигнуты. Но компания-разработчик на этом не останавливается — она продолжает продвигать свое детище на новых рынках. Ее позициям уже ничего не угрожает: она узнаваема, ее продукция пользуется стабильным спросом, доходы постепенно растут.

5. Выход, или Exit Stage. Когда компания достигает пика своего развития, инвесторы, осуществившие финансирование проекта, отказываются от своей доли в этом бизнесе и продают ее более крупным игрокам. Этот шаг приносит им хорошую прибыль. Можно сказать, ради этого момента они и вкладывают деньги в перспективное начинание. Впрочем, отдельные инвесторы сохраняют свою долю и используют ее в качестве источника постоянного дохода.

Стартап = идея + команда + финансирование

Рисунок 5.1 Компоненты стартапа

Идея — то, для чего создается стартап, команда — кем реализуется, финансирование — за счет чего.

Идея. Основным ресурсом для создания нового стартапа служит хорошая идея. Главным фактором успешности идеи является ее востребованность (степень необходимости для потребителя), ведь идея может быть необычной и новой, но пользы от нее не будет.

Команда. Команда, пожалуй, важнейшая составляющая стартапа. Если идею проекта достаточно подвергнуть формальной экспертизе, то изучению команды инвесторы уделяют огромное внимание, как и основатель проекта подбору команды для него. Зачастую команду стартапа составляют друзья, единомышленники, которые считают этот проект привлекательным и располагают необходимыми навыками и компетенциями. Важно, чтобы один член команды эффективно дополнял другого, то есть, имел те необходимые качества и навыки, которых нет у партнера. Для успешной реализации проекта

не обязателен опыт удачной реализации проектов, руководства компанией или проектами в прошлом, но, как показывает практика, подобный опыт повышает шансы на успех. Участники проекта работают в большинстве случаев за идею, условную зарплату и возможную прибыль в будущем в случае успеха, поэтому работают с огромной отдачей и по принципу «либо всё — либо ничего».

Финансирование. Стартап — это рискованный проект, который может быстро окупить вложенные в него средства, а может и провалиться. Большое количество стартапов не оправдывают возложенных на них надежд и прогорают. Удачных намного меньше. Деньги на развитие стартапа часто дают инвесторы взамен на право владения частью компании.

Любой инвестор знает, что наибольшие прибыли сулят именно «темные лошадки». Поэтому финансирование стартапов в России уже давно поставлено на поток.

Сегодня инвестициями в стартапы занимаются так называемые бизнес-ангелы и венчурные фонды. Венчурные предприниматели распоряжаются долями паевых инвестиционных фондов, которые вкладывают в молодые, но перспективные начинания. Бизнес-ангелы — это частные инвесторы, самостоятельно определяющие объект и объем инвестирования. К этим двум инвесторам стартапов можно условно добавить друзей и родственников. И как бы кому не показалось странным, но именно эта категория занимает второе место в России по объемам вложений в стартапы, а на мировом уровне — третье.

Финансирование стартапов делится на две основные категории:

– Отложенное до стабильности;
– «Веерное».

Первый тип инвестиций — вклады с прогнозируемой отдачей. Финансирование стартапа будет осуществляться на определённой стадии проекта, если проект доживёт до неё. Владельцы стартапа доходят до оговоренного уровня и получают финансирование.

Второй тип инвестирования — веерный — отличается тем, что финансирование выдаётся на ранних стадиях проекта. Инвестор финансирует проекты, которые способны окупить инвестиции в десятки раз.

Одним из самых продуктивных методов поиска инвесторов для своего проекта является «networking» — участие в отраслевых форумах и конференциях, в конкурсах стартапов и мероприятиях по венчурному инвестированию, в которых принимают участие как большое количество компаний, желающих получить финансирование, так и потенциальные инвесторы.

Привлечь инвестора может помочь публикация объявлений на соответствующих форумах и сайтах. Также существуют биржи стартапов и организации, финансирующие стартапы. В России существует несколько форм поддержки стартапов, к которым относятся государственные и частные фонды, бизнес-инкубаторы и технопарки, венчурные компании и частные инвесторы.

Привлечение в проект инвестора или инвестиций на фондовом рынке требуют от проекта открытой отчетности, контроля над финансовыми потоками, прозрачности бизнеса. Чем выше инвестиционная привлекательность предприятия, тем больше вероятность получить инвестиции.

5.2. Кейсы цифровой трансформации

Спустя 60 лет интерес к искусственному интеллекту (artificial intelligence, AI, ИИ) разгорелся с новой силой. В последнее время в сфере ИИ произошло много удивительных научных прорывов. К тому же технологии искусственного интеллекта все шире применяются на практике. Их уже давно приспособили для решения бизнес-задач. Но сейчас феномен ИИ открывается для массовой аудитории. Сервисы на базе нейросетей входят в жизнь обывателей и получают громадный виральный эффект.

Когда речь заходит о самых успешных стартапах стоит вспомнить недавний успех отечественных проектов **«Prisma»** и «Findface», а также белорусского стартапа «MSQRD».

Все это стало возможным благодаря росту производительности компьютеров, стремительному накоплению цифровых данных (а это главный учебник для ИИ) и развитию машинного обучения.

По наблюдениям агентства «CB Insights», инвестиции в ИИ сегодня бьют все рекорды. За последние 5 лет количество сделок в этой сфере выросло с 67 до 397, общий объем финансирования AI стартапов — с $282 млн до $2,4 млрд.

С начала 2016 года инвестиции привлекли больше 200 разработчиков систем искусственного интеллекта (на общую сумму около $1,5 млрд). Собственные разработки в области ИИ ведут «IBM», «Google», «Facebook», «Apple», «Samsung», «Amazon» и «Microsoft». ИТ-гиганты заинтересованы в стартапах, у которых есть разработки на базе нейросетей.

Искусственные нейронные сети разрабатываются, в том числе, чтобы понять, как работает мозг человека и пытаются воспроизвести его деятельность.

Нейросеть является обучающейся системой, которая работает по алгоритмам, а также на основе прошлого опыта. Искусственный нейрон является упрощенной моделью естественного.

Искусственно созданная нейросеть (ИНС) имитирует процесс обработки информации биологического аналога и представляет собой массив минипроцессоров, разделенный на три группы:

Таблица 5.3

Три группы минипроцессоров

Точки входа (сенсоры)	нейроны, через которые в ИНС поступает информация для обработки.
Точки выхода (реагирующие)	нейроны, через которые ИНС выдает конечный результат.
Скрытые нейроны (ассоциативные)	рабочий массив нейронов, расположенный между точками входа и выхода.

Основная работа по обработке информации происходит на уровне скрытых (ассоциативных) нейронов. Их массив упорядочен в несколько слоев, и чем больше их, тем более точную обработку данных в состоянии произвести ИНС.

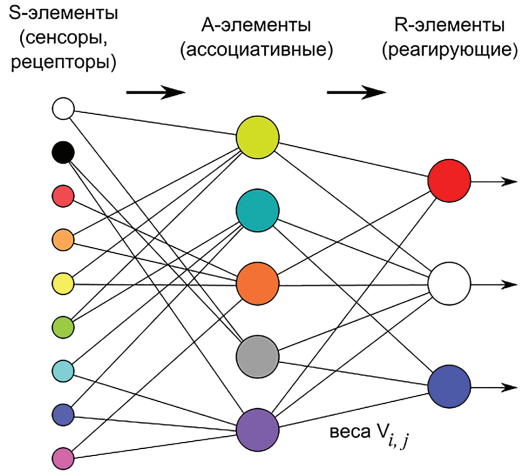


Рисунок 5.2. Схема перцептрона — простейшей однослойной нейросети

Стоит более подробно рассмотреть стартап **«Prisma»** и узнать в чем секрет его успеха.

Исследование приложения «Prisma» и ее нейронной сети

11 июня в App Store появилось приложение Prisma, которое стилизует фотографии пользователей под работы известных художников с помощью искусственной нейронной сети. Проект запустил сотрудник Mail.ru Group Алексей Моисеенков, остальные три участника проекта — выходцы из «Яндекса».

Продукт оказался на редкость виральным, опередив самые смелые ожидания основателей. За 9 дней прило-

жение стало самым скачиваемым в App Store 10 стран: России, Белоруссии, Эстонии, Молдавии, Киргизии, Узбекистана, Казахстана, Латвии, Армении и Украины. Пользователи скачали Prisma уже более миллиона раз. Стартапу сейчас приходится искусственно сдерживать рост, чтобы вычислительных мощностей хватило для обработки увеличивающегося потока изображений.

От привычных фоторедакторов Prisma отличается тем, что снимки пользователей модифицирует самообучающаяся нейросеть, а не предсказуемый алгоритм. Это далеко не первый подобный проект. Но, как говорят эксперты, Prisma первыми сумела оптимально масштабировать свой продукт для массового использования.

21 июня (всего через 10 дней после старта) стартап привлек первые инвестиции. Mail.ru Group, фонд Gagarin Capital и XBT Holding (материнская компания хостинг-провайдера Servers.com, инфраструктурного партнера Prisma) вложили в проект неназванную сумму. Условия сделки не разглашаются, но, по слухам, стартап оценили в $10 млн Знакомые с ситуацией источники сообщают, что Mail.Ru планирует внедрить Prisma для использования «ВКонтакте», в «Одноклассниках» и ICQ.

В таких фоторедакторах как Prisma и Meitu используется сверточная нейросеть, которая основана на переходе от конкретных особенностей изображения к более абстрактным деталям.

Наилучшие результаты в области распознавания лиц показала Convolutional Neural Network, или сверточная нейронная сеть (далее — СНС), которая является логическим развитием идей таких архитектур НС как когнитрона и неокогнитрона. Успех обусловлен возможностью учета двумерной топологии изображения, в отличие от многослойного персептрона.

Идея сверточной нейросети заключается в том, что каждую картинку последовательно уменьшают в размере (например, заменяя четыре соседних пикселя на один,

соответствующий их среднему значению) и заново подвергают операции свертки.

Такая нейронная сеть способна не просто обработать, а синтезировать изображение, создать его с нуля, что и делают эти нашумевшие приложения.

СНС состоит из разных видов слоев: сверточные (convolutional) слои, субдискретизирующие (subsampling, подвыборка) слои и слои «обычной» нейронной сети — персептрона.

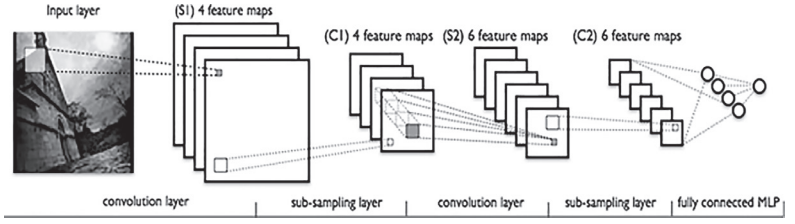


Рисунок 5.3. Топология сверточной нейронной сети

Сверточные нейронные сети обеспечивают частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям. Сверточные нейронные сети объединяют три архитектурных идеи, для обеспечения инвариантности к изменению масштаба, повороту сдвигу и пространственным искажениям.

Сверточные сети являются серединой между биологически правдоподобными сетями и обычным многослойным персептроном. На сегодняшний день лучшие результаты в распознавании изображений получают с их помощью. В среднем точность распознавания таких сетей превосходит обычные ИНС на 10—15%. СНС — это ключевая технология Deep Learning.

Основной причиной успеха СНС стала концепция общих весов. Несмотря на большой размер, эти сети имеют небольшое количество настраиваемых параметров по сравнению с их предком — неокогнитроном. Имеются варианты СНС (Tiled Convolutional Neural Network), похо-

жие на неокогнитрон, в таких сетях происходит частичный отказ от связанных весов, но алгоритм обучения остается тем же и основывается на обратном распространении ошибки. CHC могут быстро работать на последовательной машине и быстро обучаться за счет чистого распараллеливания процесса свертки по каждой карте, а также обратной свертки при распространении ошибки по сети.

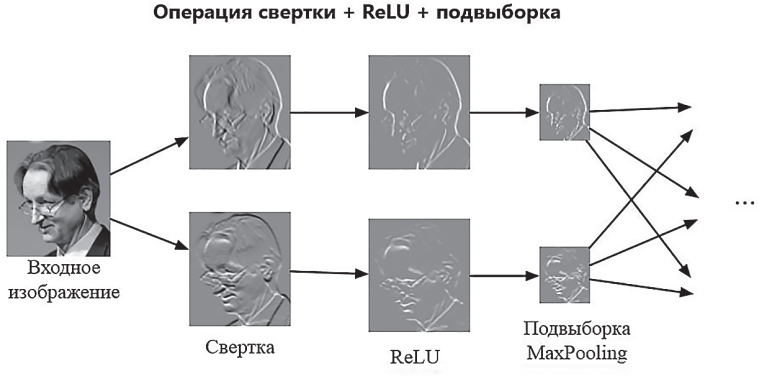


Рисунок 5.4. Пример свертки и создании подвыборки

Самые передовые идеи на 2020 год

Еще несколько лет назад список самых популярных направлений возглавляли стартапы, специализирующиеся на финтехе, e-commerce и VR/AR-технологиях. В 2019 году лидеры удерживают позиции, но наиболее перспективными отраслями становятся стартапы, ориентированные на реальную экономику, потребности человека и практические задачи бизнеса, связанные с глубокими научными исследованиями.

По данным РВК, в 2018 году инвестиции в российские стартапы, предлагающие решения для бизнеса, составили 7131,2 млн рублей. «В первую очередь это медтех: приложения и девайсы для экспресс-диагностики, контроля жизненно важных показаний, инновации в телемедицине», — говорит Александр Кузнецов, сооснователь инвестиционного фонда Russian Friends Capital.

Отдельное направление — генная инженерия, здесь лидируют американские стартапы, например Benchling, Synthego и Mammoth Bioscience.

Агротех и интеллект

Следующее востребованное направление — агротехнологии и аквакультура, то есть технологии и стартапы, позволяющие получить экологически чистые продукты питания вне зависимости от природных условий. По словам Екатерины Петровой, директора корпоративного акселератора GenerationS от РВК, инвестиции в данное направление с 2014 по 2017 год увеличились в 4 раза, со $185 млн до $877 млн, и продолжили расти в этом году. Ведущими странами в этой отрасли считаются США и Голландия. Яркий пример — канадский агростартап AquaMaof Technologies, который ежегодно поставляет 500 т атлантического лосося, выращенного в экологически чистых условиях.

Рекордсменами по объему венчурных инвестиций являются разработчики в области искусственного интеллекта (AI) и машинного обучения.

«По данным 2018 года, мировой рынок вырос более чем на 30% и превысил порог в $100 млрд в мире. По нашей оценке, российский объем инвестиций не превышает 25—26 млрд рублей в год. Среди самых крупных сделок отмечу стартапы в области искусственного интеллекта, которые получили инвестиции около $2 млрд Например, компании Pony.ai и Nuro, которые разрабатывают технологии беспилотных автомобилей, привлекли $112 млн и $92 млн соответственно», — говорит Александр Кузнецов.

«Отличный потенциал у проекта Yva нашего соотечественника Давида Яна, анализирующего действия сотрудников компаний и помогающего HR видеть, когда человек начинает выгорать на работе, и предотвращать смену

работы или уход из компании», — напоминает Станислав Мешков, генеральный директор компании Umbrella IT.

«В Китае на государственном уровне закреплен стратегический план, по которому к 2030 году будет инвестировано в развитие AI более $7 млрд, — говорит Екатерина Петрова. — Согласно CB Insight, сейчас почти половина всех венчурных сделок в Китае приходится на стартапы в сфере искусственного интеллекта». Это значит, что в Китае в стартапы такого рода инвестируют больше, чем в США.

Доставка и образование

Алексей Комаров, управляющий партнер «IT Бизнес Брокер», выделяет еще одну быстрорастущую в мире и России нишу — foodtech. Одной из заметных сделок стало инвестирование сервиса по доставке еды SaveTime: группа компаний «Ташир» выделила около 500 млн рублей на развитие проекта.

«Буквально на днях было объявлено о новом, 500-миллионном раунде в сервис по доставке продуктов Instamart, осуществленном Mail.ru и Сбербанком. На этом фоне можно ожидать конкуренции Instamart с петербургским сервисом iGooods, который привлек 123 млн от группы частных инвесторов в прошлом году», — говорит Алексей Комаров.

Максим Спиридонов, основатель и генеральный директор «Нетологии-групп», в качестве перспективной отрасли называет онлайн-образование. «В этой области интерес вызывает один из крупнейших индийских стартапов — компания BYJU'S, которая создает приложения для обучения. Именно по ней в прошлом году была закрыта крупнейшая сделка в истории EdTech в раунде $540 млн с оценкой компании в $3,6 млрд», — сказал он.

Цифровая медицина

Количество диагностируемых хронических заболеваний продолжает расти. Не дешевеют и медицинские

услуги. Плюс ко всему сохраняются проблемы с доступом к качественным специалистам для людей, живущих вдали от больших городов. В таких условиях решения в сфере цифровой медицины становятся все более популярными.

В первую очередь, речь идет о проблемах с психическим здоровьем. Например, компания Akili Interactive из США с 2014 года занимается разработкой видеоигр для пациентов с депрессией, гиперактивностью, аутизмом и рассеянным склерозом. За время работы она привлекла $120 миллионов инвестиций.

Другие участники рынка создают приложения для тех, кто борется с табачной зависимостью, нарушениями сна, диабетом и болями в спине.

Индустрия красоты

На рынке бьюти-товаров и услуг растут компании, которые предлагают индивидуальные решения. Например, стартап ModiFace помогает подобрать идеальный макияж при помощи технологий распознавания лиц и дополненной реальности. Популярный в Азии проект Sketchon предлагает печать временных татуировок с клиентским дизайном.

Персонализированное питание

Все больше людей меняют свои пищевые предпочтения, и технологические компании подстраиваются под новые потребности. Тенденция на отказ от мяса привела к появлению производителей пищи на основе растительного белка, не уступающей по вкусовым и энергетическим качествам. Ripple Foods из Калифорнии делает растительное молоко и йогурт, Beyond Meat — альтернативу мяса для вегетарианцев, New Wave Foods — креветки из растительного белка и красных водорослей.

Также активно развивается направление по подбору здоровой диеты для конкретного человека в зависимости от состояния его здоровья и генетической предрасположенности.

Киберспорт

Индустрия онлайн-игр продолжает расти. К 2021 году оборот этого рынка составит $1,65 миллиарда. Пик вложений в сервисы доставки контента прошел, когда Amazon приобрел Twitch почти за $1 миллиард. Сегодня популярны стартапы, которые помогают профессиональным геймерам улучшать их игровые стратегии. Работают такие платформы на основе искусственного интеллекта. В качестве примеров можно назвать стартап Mobalytics и российскую разработку Gosu.ai.

Микромобильность

Рост числа городского населения заставляет искать новые решения в сфере ежедневных перемещений. Параллельно с традиционным транспортом развиваются альтернативы, в том числе, и различные маркетплейсы. К примеру, международный сервис по поиску и бронированию трансферов по всему миру GetTransfer.com предлагает пользователям самим установить цену поездки и выбрать подходящий автомобиль.

За 5 лет перечень наиболее интересных для инвесторов сфер деятельности обновился. Хотя отдельные направления сохранили свою актуальность. Например, остаются популярными прорывные проекты в области кибербезопасности, мобильных приложений, “зеленых” технологий и таргетируемого e-commerce.

Один из интересных примеров — белорусский стартап Wannaby, позволяющий выбирать различные товары при помощи дополненной реальности. Начинал он с приложения для подбора лака для ногтей, интегрированного с каталогом Amazon. В конце января 2019 года вышло приложение Wanna Kicks для виртуальной примерки кроссовок. Технологии распознавания разных частей тела, за исключением лица, пока развиты достаточно слабо. Поэтому компании есть куда расти.

Большая часть инвестиций в настоящий момент приходится на проекты, связанные с Интернетом, мобильными сервисами и здравоохранением. Например, индийская компания OYO Rooms, которая специализируется на перепродаже комнат в хостелах, привлекла $1 миллиард. Ее основателя в родной стране стали сравнивать с Цукербергом.

У российских стартапов инвестируемые суммы значительно меньше, но и у них общий привлекаемый капитал растет. В 2018 году он составил $0,4 миллиарда, что на $0,15 миллиарда больше, чем годом ранее. Наиболее интересные для инвесторов отрасли — IT и медицина. Например, в ноябре 2018 года проект RealtimeBoard (платформа для совместной работы офисных команд) привлек $25 миллионов. Также можно отметить российский стартап ExoAtlet, основанный выпускниками МГУ. В него вложили $5 миллионов инвесторы из Южной Кореи (Cosmo and Company Co). Сейчас ExoAtlet — международная компания.

Вопросы для самоконтроля

1. Назовите основные стадии жизненного цикла стартапа.
2. Охарактеризуйте проект, который является стратапом.
3. Проанализируйте тенденции международного и российского рынка старапов.
4. Назовите отличительные особенности стартапов.
5. Назовите основные источники финансирования высокорискованных проектов.

Список использованных источников главы 5

1. Микаловиц М. Стартап без бюджета. — М.: МАНН, 2012. — 200 с.
2. Плосков П. Сила Instagram. Простой путь к миллиону подписчиков. — М.: Бомбора, 2018. — 240 с.

3. Тиль П. От нуля к единице. — М.: Альпина, 2018. — 192 с.

4. Бланк С., Дорф Б. Стартап. Настольная книга основателя. — М.: Альпина паблишер, 2018. — 616 с.

5. Ручкин В., Костров Б. Системы искусственного интеллекта. Нейросети и нейрокомпьютеры. — М.: КУРС, 2018. — 288 с.

6. Люгер Д. Искусственный интеллект. Стратегии и методы решения сложных проблем. — М.: ВИЛЬЯМС, 2016. — 864 с.

7. Нейронные сети для начинающих [Электронный ресурс]. — Режим доступа: https://steptosleep.ru/%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D1%81%D0%B5%D1%82%D1%8C/

8. Принцип работы свёрточной нейронной сети. [Электронный ресурс]. — Режим доступа: https://habr.com/ru/post/416777/

Глава 6
КАДРЫ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ

6.1. Задачи развития цифровой экономики

Развитие цифровой экономики связано с постановкой и решением задач в следующих направлениях: информационная инфраструктура, исследовательские компетенции и технические заделы, нормативное регулирование и информационная безопасность.

Направление ***«Информационная инфраструктура»***. К основным задачам относятся следующие.

Развитие сетей связи, способных наиболее полно обеспечить потребности по сбору и передаче данных с учетом технических требований, предъявляемых современными цифровыми технологиями.

Развитие системы центров обработки данных, способной обеспечить предоставление услуг по хранению и обработке данных на принципах доступности, устойчивости, безопасности и экономической эффективности.

Разработка информационных платформ, способной на основе облачных технологий и вычислений обеспечить потребности в работе с данными большого количества пользователей.

Создание эффективной системы получения, сбора, обработки, храненнния и предоставления пространственных данных, обеспечивая потребности в актуальной и доставерной информации о пространственных объектах (рис. 6.1)

При этом важно учитывать, что развитию данного направления припятствуют вызовы и угрозы и, прежде всего:

– угрозы, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, использующих виртуализацию, удаленные облачные хранилища данных, разнообразные технологии и устройства;

– угрозы, связанные с присутствием внешнего воздействия на информационную инфраструктуру;

– угрозы, связанные с увеличением масштабов компьютерной преступности.

Направление «***Исследовательские компетенции и технологические заделы***». Здесь основная задача — это формирование институциональной среды для проведения теоретических исследований и поддержки поисковых прикладных работ в области цифровой экономики. При этом необходимо обеспечить, во-первых, высокую эффективность научных исследований, во-вторых, высокий уровень внедрения разработок, связанных с перспективными информационными технологиями, в-третьих, технологическую независимость и конкурентоспособность по каждому направлению сквозных цифровых технологий, в-четвертых, достаточный профессиональный уровень специалистов.

Направление «***Нормативное регулирование***». В качестве основных определяются задачи формирования регуляторной среды и связанного с ней благоприятного правового режима для развития информационно-коммуникационных технологий и в дальнейшем экономической деятельности, связанной с их использованием. Поэтому их решение обеспечивает создание постоянно действующих механизмов:

– управления знаниями в области регулирования цифровой экономики,

– снятия правовых ограничений и создания правовых институтов, *направленных на формирование и* развития цифровой экономики,

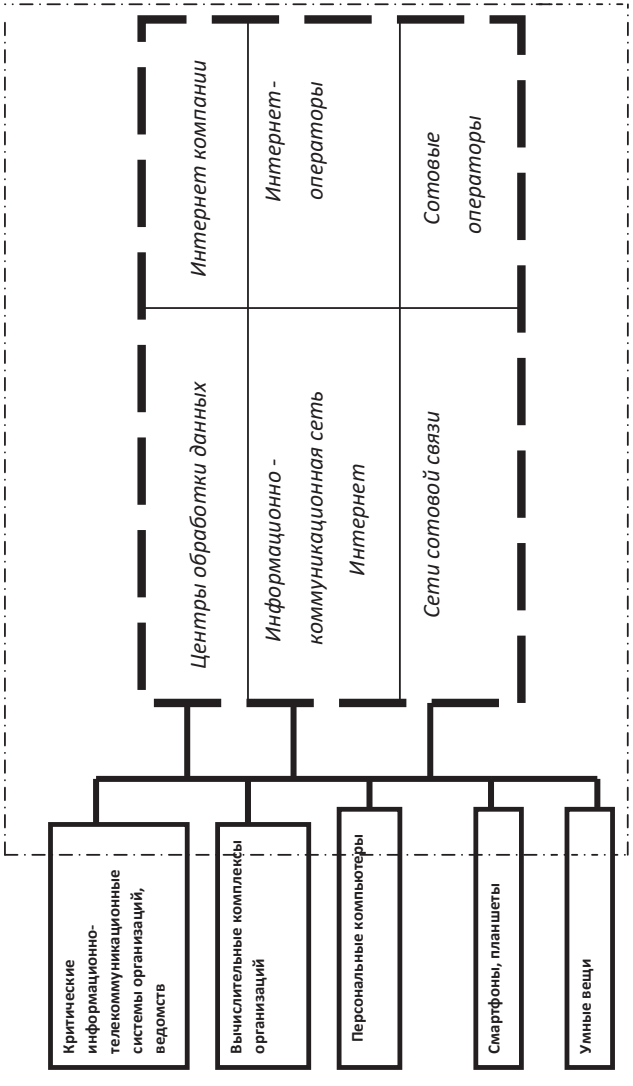


Рисунок 6.1. Область Цифровой экономики как вида экономической деятельности

– формирования комплексного законодательного регулирования отношений в сфере цифровой экономики и ее развития,

– разработки мер стимулирования деятельности по эффективному использованию современных информационно-коммуникационных технологий получения и использования данных.

Направление ***«Информационная безопасность»***. Комплекс основных задач формируется, исходя из системы основополагающих принципов, включающей:

– внедрение критических технологий, которые способны обеспечтиь целостность, конфидициальность, аутентификацию передаваемой информации и процессов ее обработки;

– использование соответствующего оборудования и систем программирования;

– применение технологий защиты информации с использовнием эффективных криптографических стандартов.

Их решение обеспечивает единство, устойчивость и безопасность информационно-телекоммуникационной инфраструктуры на всем информационном пространстве, способствует достижению состояния защищенности от внутренних и внешних информационных угроз. Тем самым создаются условия суверенитета и устойчивого развитие страны, реализации конституционных прав и свобод человека и гражданина, в том числе на достойное качество жизни.

Эффективное развития цифровой экономики в указанных направлениях возможно при высоком уровене обеспечения профессиональными кадрами, с одной стороны, и высоком уровне цифровой грамотности граждан, с другой стороны. В первом случае решается задача подготовки в необходимых объемах специалистов, обладающих соответствующим набором профессионадьных знаний, навыков и умений (компетенций), во втором — задача ценаправленного обучения населения, с одной стороны,

как производителей и потребителей информации, с другой стороны, как лиц, эксплуатирующих высокопроизводительные и многофункциональные устройства в виде персональных компьютеров, планшетов, смартфонов.

Поэтому направление ***«Кадры и образование»*** связано:

• *с созданием ключевых условий для подготовки кадров*, внедряя совершенные модели компетенций и механизмы их независимой аттестации, обеспечивая эффективное взаимодействие общества, бизнеса, рынка труда и образования;

• *с совершенствованием системы образования*, которая способна решать проблемы обеспечения цифровой экономики компетентными кадрами за счет реализации требований к ключевым компетенциям для каждого уровня образовния (общее среднее, профессиональное, доподнительное) и их приемственности;

• *с развитием рынка труда*, который должен обеспечить удовлетворение спроса на квалифицированную рабочую силу на основе масштабного использования профилей компетенций и персональных траекторий, развития трудовых и социальных отношений с гибкой и дистанционной занятностью;

• *с созданием системы мотивации,* способной обеспечить высокую заинтересованность граждан в участии в развитии цифровой экономики, освоении необходимых компетенций, а компаний — на создание и развитие соответствующих рабочих мест, включая подготовку соответствующего персонала.

6.2. Компетенции цифровой экономики

В решении вопросов кадрового обеспечения цифровой экономики решающая роль отводится моделям компетенций. Здесь под ***компетенциями*** понимается «доказанная способность использовать знания, умения, навыки, личностные качества, ценности и установки для эффектив-

ного решения определенного круга задач». Компетенции формируются в процессе целенаправленного обучения с использованием различных образовательных институтов и, в конечном итоге, представляют характеристику личности, которая заключается во владении ею системным набором компетенций, позволяющим в заданной профессиональной области решать задачи различного уровня сложности.

Системность компетенций цифровой экономики обеспечивает взаимосвязь базовых, ключевых и профессиональных компетенций, структура которой представлена на рисунке 6.1. Как можно видеть, в целостной системе определяющая роль отводится базовым компетенциям.

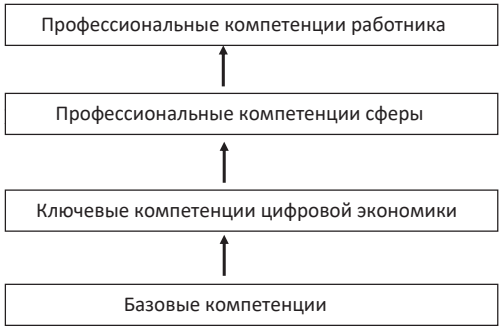


Рисунок 6.1. Схема взаимосвязи компетенций в системе компетенций цифровой экономики

Система базовых компетенций — это компетенции, универсально применяемые на протяжении всей жизни человека, во всех сферах его деятельности. Определяя саму способность к креативному мышлению, продуктивной деятельности, непрерывному саморазвитию и ответственной жизни, они составляют основу формирования профессиональных компетенций человека.

Важно понять, что набор базовых компетенций отражает отношение общества к конкретным характеристикам личности с учетом стоящих задач общественного развития. Поэтому наблюдается разнообразие в национальных подходах к их установлению, допускающее различную степень детализации.

Так, в ***Канаде*** различают 6 групп базовых компетенций: 1) критическое мышление, 2) креативность + инновационность + предпринимательство; 3) коммуникация; 4) кооперация; 5) воспитание характера (настойчивость, гибкость, ценность личностного роста); 6) гражданская грамотность как способность действовать в переменчивых и неоднозначных обстоятельствах.

В ***Финляндии*** рассматриваются базовые компетенции, объедененные в 4 группы:

1. Способы мышления (креативность, инновационность), критическое мышление, решение проблем, принятие решений.

2. Умение учиться, знание о когнитивных процессах.

3. Способность работы и коммуникация и кооперация (работа в команде); инструменты для работы, информационная грамотность.

4. Навыки для повседненевой жизни: гражданская грамотность, навыки для жизни и карьеры, профессиональная и социальная ответственность (в том числе культурная осведомленность и компетентность).

В ***Республике Корея*** речь идет о 6-ти «сквозных компетенциях XXI века»: 1) управление собой; 2) работа со знаниями и информацией; 3) креативное мышление; 4) эстетика и эмоциональность; 5) коммуникация; 6) гражданская грамотность.

Наибольший интерес представляет ***Российский атлас новых профессий***, где обозначены 11 ***надпрофессиональных навыков***:

1) экологическое мышление;
2) управление проектами;
3) системное мышление;
4) работа с людьми;
5) работа в условиях неопределнности;

6) программирование / робототехника / искусственный интелект;

7) навыки художественного творчества;

8) мультиязычность и мультикультурность;

9) межотраслевая коммуникация;

10) клиентоориентированность;

11) бережливое производство.

Опираясь на соответствующий набор базовых компетенций, формируется система ***ключевых цифровых компетенций***, распространяющаяся на цифровую экономику. Как единая система профессиональных компетенций цифровой экономической деятельности, она актуальная для данных социально-экономических условий и устанавливает единые требования к процессам и результатам образования, с одной стороны, и квалификациям работников, с другой стороны.

Из международного опыта наибольший интерес представляет система ключевых цифровых компетенций, которая разработана в исследовательских структурах ***Европейского Союза*** (таблица 6.1).

При этом для каждой компетенции определяется 4 уровня квалификации, каждый из которых имеет два подуровня.

6.3. Система уровней квалификаций для цифровых компетенций

Базовый уровень

Выполнение определенных операций в конкретной области компетенций под руководством специалиста.

Самостоятельное выполнение определенных операций в конкретной области компетенций и привлечение специалиста в случае необходимости.

Промежуточный уровень

Самостоятельное выполнение определенных операций в конкретной области компетенций и непосредственное решение возникающих задач.

Таблица 6.1

Концептуальная схема цифровых компетенций для граждан ЕС

Области компетенций				
1. Грамотность в области информации и данных	2. Коммуникация и сотрудничество	3. Создание цифрового контента	4. Безопасность	5. Решение проблем
1.1. Просмотр, поиски фильтрация данных информации цифрового контента	2.1. Взаимодействие с помощью цифровых технологий	3.1. Разработка контента — создание и редактирование цифрового контента в разных форматах	4.1. Защита устройств и цифрового контента, а также понимание рисков и угроз в цифровых средах	5.1. Решение технических проблем при работе с устройствами и использованием цифровых технолгий
1.2. Оценка дезинформации и цифрового контента	2.2. Совместное использование различных ресурсов с помощью цифровых технологий	3.2. Интеграция цифрового контента в существующую совокупность знаний и его переработка для создания нового оригинального и ревалентного контента и знаний	4.2. Защита персональных данных и конфиденциальность	5.2. Определение потребностей и технологических решений для их удовлетворения путем выявления оценки выбора и использования цифровых инструментов настройки цифровых сред для личных нужд

Окончание таблицы

Области компетенций				
1.3. управление данными информацией и цифровым контентом	2.3. Участие в жизни общества посредством цифровых технологий государственных и частных цифрровых услуг	3.3. Авторские права и лицензии — понимание того, как они применяются к данным цифровой информации и контенту	4.3. Защита здоровья и благополучия, навыки парирования рисков для здоровья и угроз физическому и психологическому благополучию при использовании цировых технологий	5.3. Творческое использование цифровых технологий для производства знаний и инноваций, разрешения проблемных ситуаций в цифровых средах
	2.4. Сотрудничество с использованием цифровых технологий для совместного создания данных ресурсов и знаний	3.4. Программирование для решения конкретной проблемы или выполнения конкретной задачи	4.4. Защита окружающей среды на основе учета экологического воздействия цифровых технологий и их использования	5.4. Индентификация пробелов в цифровых компетенциях для улучшения и актуализации собственных навыков в процессе цифровой эволюции, помощи другим, а также для саморазвития
	2.5. Сетевой этикет			
	2.6. Управление цифровой индентичностью			

Самостоятельное выполнение определенных операций в конкретной области компетенций в соответствии собственными потребностями и решение для этого как четко определенных, так и нестандартных задач.

Продвинутый уровень

Руководство другими при выполнении определенных операций в конкретной области компетенций, демонстрация возможностей различных технологий, предложение различных способов решения задач.

Выполнение определенных операций в конкретной области компетенций в соответствии с собственными потребностями и потребностями других, в том числе в сложных обстоятельствах.

Высокоспециализированный уровень

Определение путей решения сложных проблем в конкретной области компетенций в условиях ограниченной информации, саморазвитие через отслеживание новых разработок, внесение собственного вклада в профессиональную деятельность и развитие цифровых компетенций у других.

Решение комплексных многофакторных проблем в конкретной области компетенций, нахождение возможностей для саморазвития, следование в русле цифровой эволюции, продложение сообществу новых идей и процессов.

Другим примером системы ключевых компетенций для цифровой экономики служит сформировавшийся в рамках ***G20*** подход к измерению цифровой грамотности, основанный на рассмотрении признаков знаний, навыков и умений в конкретных аспектах, начиная с информационной грамотности до отношений к технологическим новациям (таблица 6.2).

В нашей стране с принятием Постановления Правительства «Программа “Цифровая экономика Россий-

ской Федерации”» активизировалась работа в области формирования ключевых компетенций для цифровой экономики, на основе которых будут разрабатываться пофессиональные стандарты, а затем и стандарты образовательные. Одним из вариантов станет разработка, в основу которой положена система ключевых компетенций, предложенная Национальным центром цифровой экономики и представленная в таблице 6.3.

Источниками получения каждой из перечисленных в рамках данной схемы компетенции являются: семья, государство (в части создания соответствующей политической, правовой и деловой среды, реализации государственных программ и проектов), школа, колледж, вуз, курсы, работа, СМИ, самообразование, индивидуальный эксперт. Как показывает анализ, наиболее весомыми источниками приобретения компетенций выступают самообразование, колледж и вуз (удельный вес от 13,1% до 13,4%), а также работа (13,0%). Несколько меньший удельный вес у школы (10,7%), обучающих курсов — курсов дополнительного образования (10,5%), индивидуальных экспертов (8,8%). Роль семьи, СМИ и государства еще меньше, но это не снижает их значимость с системе формирования компетенций для цифровой экономики.

Таблица 6.2

Явления цифровой грамотности, подлежаие оценке согласно методологии G20

Аспект	Знания	Навыки	Умения
Информационная грамотность	Понимание роли и степени влияния информации на жизнь человека	Умение искать и находить информацию в разных ресурсах	Понимание пользы и вреда информации

Окончание табл. 6.2

Аспект	Знания	Навыки	Умения
Компьютерная грамотность	Понимание технических составляющих компьютера и принципов их взаимодействия	Легкость в использовании цифровых устройств вне зависимости от платформ/интерфейса	Понимание «предназначения» компьютера и целей его использования
Медиаграмотность	Понимание многообразия источников информации, форм и каналов ее распространения	Умение искать новости в разных источниках, проверять их полноту и доставерность	Критическое отношение к сообщениям, новостям
Коммуникационная грамотность	Понимание отличия цифровых коммуникаций от живого общения	Умение использовать современные средства коммуникаций (социальные сети, мессенджеры)	Осознание наличия особой этики и норм общения в цифровой среде
Отношение к технологическим новациям	Понимание технологических трендов	Готовность работать с новыми и современными технологиями (приложениями, гаджетами)	Понимание пользы технологических инноваций как для развития общества, так и для себя лично

Профессиональный стандарт специалиста

Система ключевых компетенций цифровой экономики ложатся в основу разработки профессиональных стандартов для конкретных видов занятости. Согласно нормативным

Таблица 6.3

Концептуальная схема ключевых компетнций для цифровой экономики

Способ мышления	Способ работы	Навыки для работы			
		Деловые навыки	**Коммуникативные навыки**	**Информативные навыки**	**Цифровые/технические навыки**
Настойчивость	Коммуникация	Лидерство	Навыки межличностной коммуникации	Навыки поиска и фильтрации информации	Компьютерная и ИТК-грамотность: – умение работать с устройствами – понимание основный ИТК-концептов – способность выбирать нужные настройки (устройств и сервисов) – умение работатьс файлами
Стойкость	Кооперация	Умение работать в условиях неопределенности	Навыки межотраслевой коммуникации	Навыки оценки данных, их источников и ревалентности (включая медиаграмотность)	Стандартные цифровые навыки: – управление цифровой/сетевой индентичностью
					– умение защищать свои устройства и информацию от вирусов и злоумышленников – использование офисного ПО – использование корпоративного ПО
Гибкость	Креативность, творческий подход	Навыки управления : – людьми – проектами – вниманием	Навыки цифровых коммуникаций: – нетворинга – совместного использования ресурсов	Навыки обработки информации	Продвинутые цифровые навыки: – програмирование – разработка приложений – администирование сетей – использование отраслевых программ – владение технологиями искусственного интелекта,

Продолжение табл. 6.3

Способ мышления	Способ работы	Навыки для работы			
		Деловые навыки	**Коммуникативные навыки**	**Информативные навыки**	**Цифровые/технические навыки**
					индустриального интернета, интернета вещей, и др. робототехникой
Умение принимать решения и решать проблемы	Инновационность	Навыки кооперации: –умение выстраивать партнерские отношения –умение работать в команде		Навыки организации и хранения данных	Способность решать возможные проблемы с помощью цифровых инструментов
Критическое мышление	Предприимчивость	Навыки в области развития бизнеса: –продаж и маркетинга –выведения продуктов и услуг		Навыки анализа и использования данных	Творческое использование цифровых технологий для производства знаний и инноваций
		на рынок –инвестирования			
Социальная ответственность –гражданская грамотность –экологическое мышление	Клиентоориентированность	Навыки цифрового предпринимательства		Способность создавать цифровой контент	Знание сетевого этикета
Нацеленность на личный рост	Бережливое производство	Идентификация проблем в цифровых компетенциях для актуализации собственных навыков и помощи другим		Навыки интеграции цифрового контента в соответствующую совокупность знаний	Участие в жизни общества с помощью цифровых технологий
Умение учиться, постоянное обучение				Навыки использования цифровых приложений и услуг	
Правовое мышление				Правовая грамотность: –знание основ авторского	

Окончание табл. 6.3

Способ мышления	Способ работы	Навыки для работы			
		Деловые навыки	**Коммуникативные навыки**	**Информативные навыки**	**Цифровые/технические навыки**
				и лицензионного права	
Позитивное / конструктивное отношение к технологическим инновациям				–знание правовых актов, регулирующих использование интернета –умение обращаться с персональными данными	
Эстетика и эмоциональность					
Мультиязычность и мультикультурность					

документам «профессиональный стандарт как характеристика квалификации, необходимой для осуществления профессиональной деятельности — это многофункциональный нормативный документ, определяющий в рамках конкретного вида (области) профессиональной деятельности требования к содержанию и условиям труда, квалификации и компетенциями работников. Нацеленный на описание особенностей квалификации, он с позиций сферы труда, объединений работодателей и профсоюзных сообществ через трудовые функции и трудовые действия раскрывает цель и содержание вида профессиональной деятельности, место в системе уровней квалификаций, требования к образованию и обучению, опыту практической работы, необходимым знаниям и умениям работника. И как следствие, профессиональный стандарт является продуктом профессионального сообщества, отражая договоренности с участниками рынка и создавая конкурентную среду».

Важнейшей функцией профессиональных стандартов является связь между требованиями труда и системой образования. На основе утвержденного профессионального стандарта формируются и обновляются федеральные государственные образовательные стандарты, проектируются учебные планы подготовки специалистов в системах бакалавариата, специалитета, магистратуры, дополнительного профессионального обучения, а в последующем — разработка основных профессиональных образовательных программ.

Темпы развития цифровой экономики за счет широкого внедрения цифровых трансформаций, технологической базой которых выступают информационные системы, в наибольшей степени будут определять специалисты по информационным системам и информационным технологиям.

Рассматривая проблемы совершенствования деятельности специалиста по информационным системам, следует учитывать, что ее эффективность в случае цифровой

экономики будет определяться взаимодействием со специалистами по информационным ресурсам. Важность этого взаимодействия во многом определяется тем, что, если специалист по информационным системам решает вопросы в части ***«как сделать»***, то специалист по информационным ресурсам связан с проблемами ***«что делать»***.

Разработка и утверждение ключевых компетенций для цифровой экономики потребует как пересмотра действующих профессиональных стандартов, так и разработки новых.

В частности, речь идет о профессиональном стандарте специалиста по цифровой экономике, профессиональная деятельность которого связана с созданием и управлением экосистемой цифровой экономики. Оснавная цель этого вида деятельности будет заключаться в разработке (модернизации) и управлении информационными платформами для обеспечения необходимого спектра информационных услуг, включая услуги по производству востребованной информации по запросам организаций и физических лиц.

В разработке такого профессионального стандарта должны найти отражение ключевые компетенции, представленные выше в виде концептуальной схемы. Эти компетенции вносят новации в части деловых, информационных и цифровых/технических навыков.

В части ***деловых навыков***, наряду с коммуникационными навыками, навыками креативности и инновационности, особое внимание необходимо уделять формированию предпринимательских навыков, а именно: цифровое предпринимательство, навыки в области продаж, маркетинга, нетворнига и развития бизнеса, навыки вывода информационного продукта и услуг на рынок.

В части ***информационных навыков*** речь идет об умении:

- оценивать источники информации и их релевантность,
- работать с персональными данными,

- защищать свои устройства и информацию от вирусов и злоумышленников,
- полноценно существовать в цифровом обществе и эффективно пользоваться онлай-приложениями и услугами-месенджерами, финансовыми сервисами, соцсетями, порталами госуслуг и т. п.;
- решать возникающие проблемы с помощью цифровых инструментов.

В области ***цифровых/технических навыков*** при развитии компьютерной и ИТК-грамотности формировать навыки:

- использования технологий SMAAC (социальные сети, мобильная связь, приложения, Big-data-аналитика, облачные технологии),
- использования цифровых технологий в отраслевых и корпоративных программах повышения производительности ресурсов,
- использования цифровых коммуникаций — сотрудничества в проектах,
- владения технологиями индустриального интернета вещей.

Вопросы для самоконтроля

1. Перечислите ключевые компетенции цифровой грамотности.
2. Какова роль профессиональных стандартов в формировании компетенций цифровой экономики?
3. Какие мероприятия запланированы в целях совершенствования цифровой экономики при подготовке школьников?
4. Какие мероприятия запланированы для обучения ИТ-специалистов?
5. Какая доля населения страны, согласно плану федеральной программы должна обладать цифровыми навыками?

Список использованных источников главы 6

1. Программа «Цифровая экономика Российской Федерации»: [Электронныйресурс] // Правительство РФ. — М., 2018. — URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf/ (Дата обращения: 28.10.2019).

2. Указ Президента России от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»: [Электронныйресурс] — URL: http://www.kremlin.ru/acts/bank/43027 (Дата обращения: 28.10.2019).

3. Концепция и дорожная карта НСУД: [Электронный ресурс] — URL: https://digital-api.ac.gov.ru/upload/iblock/53c/Концепция и дорожная карта НСУД.PDF. (Дата обращения: 28.10.2019).

4. Прохоров А., Коник Л. Цифровая транформация. Анализ, тренды, мировой опыт. — М.: ООО «Альянс-Принт», 2019. — 368 с.

5. Михненко О.Е Цифровая экономика: что это такое? // Автоматика, связь информатика на железнодорожном транспорте. — 2018. — №1 — С. 6—10.

6. Михненко О. Е. Цифровые технологии и эффективность статистических показателей // Цифровая трансформация в экономике транспортного комплекса: Материалы международной научно-практической конференции / Под ред. Ю. И. Соколова, Г. В. Бубновой, Л. А. Каргиной, И. А. Епишкина. — М.: РУТ (МИИТ), 2019. — С. 207—216.

ПРАКТИКУМ

Методические указания по написанию рефератов

Реферат представляет собой доклад на определенную тему в виде обзора соответствующих литературных и других источников или краткое изложение книги, статьи, исследования с основными фактическими сведениями и выводами.

Написание реферата используется в целях приобретения студентом необходимой профессиональной подготовки, развития умений и навыков самостоятельного научного поиска: изучения библиографических источников по выбранной теме, их анализа и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. На основе тщательного анализа и обобщения научного материала в реферате сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов и выводов.

Основными задачами написания реферата являются:

– закрепление и расширение теоретических знаний, полученных на лекциях и семинарах, а также систематизация этих знаний;

– обучение навыкам самостоятельной работы с основной и дополнительной литературой;

– умение самостоятельно систематизировать и излагать знания, полученные в процессе самостоятельного изучения литературы;

– самостоятельное, углубленное изучение вопросов, заинтересовавших студента.

Задание на реферат выдается студенту по его желанию в соответствии с индивидуальным планом обучения как форма контроля освоения изученного материала.

Темы рефератов, которые предложены в учебнике, охватывают основные проблемы курса. Студент при желании может сам предложить ту или иную тему, предвари-

тельно согласовав ее с преподавателем. После этого необходимо изучить нормативные акты, литературные и иные источники, рекомендованные преподавателем или самостоятельно подобранные в результате изучения материалов по теме в библиотеке.

Реферат, как правило, состоит из *введения,* в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, в котором формируются выводы, оценки, предложения.

Изложение материала в реферате должно быть кратким, точным, последовательным, отражающим объект и предмет изучения. Рекомендуется включать в реферат схемы, рисунки и таблицы, помогающие раскрыть основное содержание проблемы и сократить объем работы. Сноски должны быть полными: с указанием фамилии и инициалов автора, названия книги, места и года ее издания, страницы, с которой взята цитата или соответствующее положение. Для научных статей из журналов, сборников в сносках указывают фамилию и инициалы автора, название статьи, затем название журнала или сборника статей с указанием года издания и номера (или выпуска).

Объем реферата — от 10 до 20 машинописных страниц. На титульном листе студент указывает название вуза, кафедры, полное наименование темы реферата, свою фамилию и инициалы, а также ученую степень, звание, фамилию и инициалы научного руководителя.

Примерная тематика рефератов

1. Цифровая экономика и экономический рост.
2. Технологическое развитие: исторические вехи и современность.
3. Четвертая промышленная революция и информационная глобализация.
4. Основные характеристики и возможности информационной (сетевой) экономики.

5. Распределенные вычисления и хранилище данных (облачное хранение).
6. Роль «больших данных» в принятии решений в экономике и финансах.
7. Интернет вещей.
8. Экономические основы технологии распределенных реестров хранения информации. Преимущества и проблемы применения блокчейна.
9. Трансформация промышленности в цифровой экономике.
10. Киберфизические системы, технологии PLM, 3D-печать.
11. «Умные» производства.
12. Цифровая логистика: «умные» контейнеры и склады, дроны, беспилотные грузовые самолеты и автомобили.
13. Цифровая железная дорога.
14. Природа информационного товара: информационный продукт и информационная услуга.
15. Развитие систем электронных платежей. Интернет-банкинг.
16. Виды электронной коммерции. Особенности сделок в цифровой среде.
17. Электронная (мобильная) торговля.
18. Бизнес в сети Интернет. Интернет-магазины.
19. Особенности современного рынка финансовых технологий. Цифровая трансформация финансовых услуг.
20. Влияние финансовых технологий на развитие банковской сферы.
21. Перспективы развития банковского сектора в условиях внедрения современных финансовых технологий.
22. Цифровизация страхового рынка.
23. Цифровые риски. Проблемы цифровой безопасности.
24. Трудовая деятельность в условиях цифровой экономики.
25. Изменение функций государства в цифровой экономике.
26. Концепция «электронного правительства».

27. Государственные информационные ресурсы.

28. Электронное здравоохранение.

29. «Цифровое законодательство» Российской Федерации.

30. Цифровая повестка Евразийского экономического союза.

31. Создание Единого цифрового рынка ЕС.

32. Формирование системы показателей для рейтинговой оценки развития цифровой экономики.

33. Основные индексы, характеризующие развитие цифровой экономики в странах мира.

34. Современное состояние ИТ-отрасли (для разных стран).

35. Оценка развития цифровой экономики в Российской Федерации.

Примерные вопросы к экзамену

1. Информация как экономическое благо и фактор производства.

2. Сущность информационно-коммуникационных технологий.

3. Влияние информационно-коммуникационных технологий на глобализацию мировой экономики.

4. Понятие цифровой экономики.

5. Структура цифровой экономики. Субъекты, объекты и институты цифровой экономики как системы.

6. Цифровая экономика и экономический рост.

7. Технологическое развитие: исторические вехи и современность.

8. Четвертая промышленная революция и информационная глобализация.

9. Основные характеристики и возможности информационной (сетевой) экономики.

10. Влияние информационной экономики на участников рынка (покупатели, производители, структура коммерческих отношений).

11. Цифровая экономика как дальнейшее развитие информационной (сетевой) экономики и новая стадия глобализации.

12. Распределенные вычисления и хранилище данных (облачное хранение).

13. Роль «больших данных» в принятии решений в экономике и финансах.

14. Интернет вещей.

15. Экономические основы технологии распределенных реестров хранения информации (блокчейн).

16. Преимущества и проблемы применения блокчейна.

17. Криптовалюты: история, классификация и правовое регулирование.

18. Перспективы и риски применения систем распределенного реестра.

19. Трансформация промышленности в цифровой экономике.

20. Киберфизические системы, технологии PLM, 3D-печать.

21. «Умные» производства.

22. Цифровая логистика: «умные» контейнеры и склады, дроны, беспилотные грузовые самолеты и автомобили.

23. Природа информационного товара: информационный продукт и информационная услуга.

24. Развитие систем электронных платежей. Интернет-банкинг.

25. Виды электронной коммерции. Особенности сделок в цифровой среде.

26. Электронная (мобильная) торговля.

27. Бизнес в сети Интернет. Интернет-магазины.

28. Особенности современного рынка финансовых технологий. Цифровая трансформация финансовых услуг.

29. Влияние финансовых технологий на развитие банковской сферы.

30. Трансформация внутренней и внешней среды бизнеса в условиях цифровой экономики.

31. Характер конкуренции в цифровой экономике.

32. Цифровые риски. Проблемы цифровой безопасности.

33. Изменение характера и типа трудовой деятельности в условиях цифровой экономики.

34. Децентрализация трудовой деятельности во времени и пространстве.

35. Формирование сетевых форм деятельности и горизонтальных структур взаимодействия субъектов рынка труда.

36. Изменение роли и функций государства в цифровой экономике.

37. Концепция «электронного правительства».

38. Государственные информационные ресурсы.

39. Электронное здравоохранение.

40. «Цифровое законодательство» Российской Федерации.

41. Основные индексы, характеризующие развитие цифровой экономики в странах мира.

Задания к практическим занятиям по теме «Цифровые технологии»

1. Организовать добавление новых ресурсов Azure (New, Storage-Storage account, задать имя аккаунта <Name>. core.windows.net, тип модели — Resource Manager, тип Storage (general purpose v1), уровень производительности — Standart, режим репликации — Locally-Redundant storage (LRS). Для обеспечения «бесшовного» обновления ключей использовать ключи key1 и key2). Организовать облачное хранение в Microsoft Azure Storage. В облачном сервисе Queue Storage произвести обмен сообщениями и синхронизацию распределенных приложений, в сервисе Table Storage организовать базу данных NoSQL.

2. Организовать работу с хранилищем BLOB с помощью веб-портала, добавить контейнер +Container, имя pokercomm, уровень доступа Private (no anonymous access), загрузить файл в контейнер по ссылке Upload, настроить политику доступа к контейнеру через вкладку

Access policy, добавить новую шару +File share, добавить имя шары pokerfileshare и размер её 10Гбайт. Шара отличается от контейнера тем, что для неё устанавливается квота — верхний предел размера. Доступ к шаре возможен по протоколу SMB 3.0 и может быть примонтирован к виртуальным машинам (File Storage, ссылка Connect).

3. Создать бакеты и организовать манипулирование объектами между ними с применением сервиса AWS S3: +Create bucket, вкладка Name and region.

4. Организовать реляционное хранилище информации с определенными значениями размера и максимального DTU. Для создания экземпляра Azure SQL необходимо выбрать ссылку+New, ссылка SQL-Database, имя базы данных pokerexampleclient, группа ресурсов PockerRumExample, источник базы Blank database. Указать имя сервера — pokerexample, учетные данные — Server admin login и Password, пользователь администратор и его местоположение — Central US, ценовой уровень Pricing tier. Для получения доступа к базе данных извне подключить строку подключения с учетными данными пользователя — Connecting string.

Провести мониторинг базы данных — DTU, проанализировать закономерности в функционировании базы данных, суточные пики и провалы активности или загруженности базы по дням недели. Это необходимо для определения, является ли текущий ценовой уровень оптимальным или необходимо его изменить.

В облачных средах реляционные базы данных представлены в трех видах: SQL as Service — бессерверный сервис, как готовые образы для виртуальных машин и как Docker-образы, развернутые в кластерах AWS ECS или Azure Service Fabric.

5. Организовать работу с нереляционными базами данных: DocumentDB и MongoDB (документоориентиро-

ванные), Gremlin (графовая база данных), Table (таблица типа «ключ — значение»), Cassandra (база данных, относящаяся к типу семейства столбцов).

Создать аккаунт CosmosDB, +New, CosmosDB. Указать идентификатор аккаунта (ID), выбрать его тип (API), группу ресурсов (Resource Group), местоположение и включить опцию географического дублирования (Enable geo-redundancy). Перейти на вкладку Overview: на карте показаны доступные для репликации регионы (прозрачные шестиугольники) и регионы, использованные в настоящий момент (закрашенные шестиугольники). Добавить коллекцию +Add Collection: создать первую базу данных (Database id) — PockerGameData, создать коллекцию (Collection id) — GameEvents. Выбрать размер хранилища (Storage capacity). Заполнить таблицу данными: Items, Create, ввести поля в появившуюся форму.

6. Проработать доставку BigData в облако: Event Hub, IoT Hub, Apache Kafka, Azure Event Hub +New — открытие информационной страницы сервиса, заполнить первоначальную форму настройки Event Hub, создать пространство имен mainGameConcentrator, выбрать ценовой уровень Pricing tier: Basic и Standard, указать группу ресурсов PockerRumExample, местоположение — Central US и одну единицу пропускной способности, снять флажок в Enable auto-inflate, определить верхний предел в поле Specify Upper Limit. На открывшейся странице рассмотреть метрики для заданных временных интервалов. Создать экземпляр Event Hub: +Event Hub, дать имя mainhub вновь создаваемому концентратору, количество разделов поставить минимальным — 2, ценовой уровень Basic, время жизни сообщений — retention period, включить захват сообщений capture — недоступный, сконфигурировать настройки политики совместного доступа Shared access policies: +Add, SendReadAccess, снять флажок Send и Listen, Create.

7. Провести сравнительный анализ фреймворков, пакетных анализов данных: Hadoop, Apache Pig YARN, HDFS, MapReduce, Apache Hive.

8. Автоматизировать работу копирования и трансформации данных в среде AWS Data Pipeline: Create new pipeline (создать новый конвейер), указать источники файла конвейера, вариант конфигурирования Data Factory для копирования данных из таблицы Poker Events Dynamo DB в папку S3, указать регион, где расположена таблица us-east-2, в поле Schedule указать тип запуска. Результаты работы конвейера отображается на панели списка конвейера List Pipelines.

ЦИФРОВАЯ ЭКОНОМИКА

Учебник

под редакцией доктора экономических наук,
профессора *Л. А. Каргиной*

Публикуется в авторской редакции
Корректура *Назарова Н. Н.*
Дизайн обложки *Вершинина И. А.*
Компьютерная верстка *Вершинина И. А.*

Издательство «Прометей»
119002, г. Москва, ул. Арбат, д. 51, стр. 1
Тел./факс: +7 (495) 730-70-69
E-mail: info@prometej.su

Подписано в печать 00.00.2020
Формат 60×84/16. Объем 13,75 п.л.
Тираж 500 экз. Заказ № 000