ГУАП

КАФЕДРА №

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ _____

ПРЕПОДАВАТЕЛЬ

должность, уч. степень, звание		подпись, дата		инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №

Вариант

по курсу:

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №					
			подпись, дата		инициалы, фамилия

Санкт-Петербург 2025

СОДЕРЖАНИЕ

1 Введение

Информационные технологии (IT) в России за последние годы стали важным драйвером экономического роста. С увеличением числа компаний-разработчиков программного обеспечения и экспорта IT-продуктов отрасль демонстрирует устойчивость даже в условиях экономических вызовов, таких как пандемия. Доходы российских софтверных компаний выросли с 3,6 млрд долларов в 2015 году до 17,7 млрд долларов в 2024 году. Этот рост требует надежной законодательной базы, которая поддерживает инновации, но также защищает национальные интересы.

1.1 Основные законы и регулирующие органы

Фундаментом правового режима для всей российской цифровой экосистемы остается Федеральный закон “Об информации, информационных технологиях и о защите информации” № 149-ФЗ от 27 июля 2006 года [1]. Он формулирует базовые понятия “информация”, “информационная система” и “владелец информации”, уточняет, какие сведения относятся к ограниченному доступу, и закрепляет принцип приоритета безопасности при любой обработке данных. В развитие этих норм действует четвертая часть Гражданского кодекса РФ [2], охватывающая патентное право, товарные знаки и смежные категории интеллектуальной собственности, что критически важно для программного обеспечения, баз данных и алгоритмов. Персональные данные регулируются Федеральным законом № 152-ФЗ [3], который определяет, какие действия считаются обработкой, обязывает операторов иметь публичную политику конфиденциальности и вводит концепцию согласия субъекта. Сегмент рекламы в интернете подпадает под Федеральный закон “О рекламе” № 38-ФЗ [4], требующий, чтобы цифровая реклама была прозрачна, достоверна и проверялась на наличие запрещенного контента. Телеком-аспекты, включая присоединение к сетям связи общего пользования, порядки лицензирования и универсальное обслуживание, регулируются Законом “О связи” № 126-ФЗ [5]. Наблюдение за исполнением всех упомянутых актов возложено главным образом на Роскомнадзор, который ведет реестр запрещенных сайтов, тогда как ФСБ курирует защиту государственной тайны и сертифицирует средства криптографической защиты в порядке, установленном Указом Президента № 250 от 1 мая 2022 года [8].

2 Ключевые особенности

2.1 Закон о Рунете и суверенный интернет

Федеральный закон № 90-ФЗ от 1 мая 2019 года [6], прозванный “Законом о Рунете”, вступил в силу 1 ноября 2019 года и ввел принцип технологического суверенитета российского сегмента сети. Операторы связи обязаны установить технические средства противодействия угрозам, которые по факту реализуют глубинный анализ пакетов и позволяют централизованно управлять трафиком. Роскомнадзор получил правомочия издавать инструкции о маршрутизации, проводить стресс-тесты и отключать внешние шлюзы при возникновении чрезвычайной ситуации. На уровне инфраструктуры создана дублирующая система национальных доменных серверов, что обеспечивает автономность DNS-зоны RU и РФ в случае внешней блокировки. Практика последних лет показала, что эти меры используются не только во время кибератак, но и для исполнения судебных решений о блокировке запрещенного контента, а также при ограничении работы отдельных иностранных сервисов; критики указывают, что подобная концентрация контроля повышает риски избыточной цензуры, в то время как сторонники подчеркивают значимость защищенности критической цифровой инфраструктуры.

2.2 Предустановка российского программного обеспечения

С 1 апреля 2021 года все смартфоны, ноутбуки, смарт-ТВ и иные устройства, официально поставляемые в Россию, должны иметь предустановленные отечественные приложения, перечень которых утверждается Минцифры и регулярно актуализируется распоряжениями правительства . В список обычно входят браузер, почтовый клиент, офисный пакет, антивирус и маркетплейс, разработанные российскими компаниями или прошедшие сертификацию как совместимые с национальными сервисами. Производителю предоставляется право выбора конкретного продукта, однако отсутствие любой из обязательных категорий карается штрафами, приостановлением деклараций о соответствии и отзывом партии товара из оборота. Потребители сохраняют возможность удалять или заменять такие программы, что формально соблюдает принцип свободы выбора, но на практике резко повышает видимость локальных брендов и снижает барьер входа для разработчиков. Наиболее заметный рыночный эффект - рост доли российских

почтовых и картографических сервисов в мобильном сегменте, а также ускоренный переход некоторых вендоров к выпуску модифицированных прошивок, чтобы соответствовать требованиям без потери доступа к глобальным магазинам приложений. Закон вписывается в стратегию импортозамещения и цифрового суверенитета, формируя устойчивый спрос на отечественные ИТ-продукты и сервисы поддержки.

2.3 Ограничения на иностранное программное обеспечение

Постановление Правительства № 1236 от 16 ноября 2015 года [7] запрещает госорганам и учреждениям приобретать иностранное ПО, если в реестре российского ПО есть эквивалентное решение . При выборе продукта заказчик обязан обосновать отсутствие функциональных аналогов либо доказать, что отечественный софт не соответствует критически важным требованиям; такая экспертиза проводится под контролем Минцифры. Исключения допускаются для программ, зашитых в специализированное оборудование, систем промышленной автоматизации и случаев, когда переход приведет к угрозе информационной безопасности или остановке технологического процесса. Для поддержки исполнителей внедрены субсидии на сертификацию и адаптацию ПО, а с 2024 года действует льготный режим НДС для отечественных разработчиков, что должно сократить издержки бюджетного сектора на лицензии. С другой стороны, бизнес-сообщество отмечает, что за шесть лет реализации нормы уровень совместимости российских решений с международными экосистемами вырос, но не всегда достаточен для высоконагруженных корпоративных систем, из-за чего часть закупок переводится в категорию исключений, а рынок остается сегментированным.

2.4 Локализация персональных данных

Поправки к Закону о персональных данных, вступившие в силу 1 сентября 2015 года, установили требование хранить и обрабатывать персональные данные россиян преимущественно на территории РФ. Операторы обязаны обеспечить первичную запись таких данных на российские серверы, а любая трансграничная передача допускается только при соблюдении перечня условий, включая адекватный уровень защиты в стране-получателе. За нарушение предусмотрены штрафы до 18 млн руб. и возможность блокировки ресурса; в резонансных делах против крупных соцсетей применялась именно

блокировка, которая позднее снималась после частичного выполнения требований. Закон стимулировал открытие дата-центров международными корпорациями в Москве, Санкт-Петербурге и Казани, а также появление ряда локальных облачных провайдеров, ориентированных на compliance-услуги. Параллельно с 2022 года действует институт “data-анкоры”, когда данные могут копироваться в защищенные узлы, что облегчает компаниям гибридную эксплуатацию зарубежных сервисов без нарушения территориального принципа.

2.5 Регулирование социальных сетей и распространения информации

Изменения в статью 10.6 Закона № 149-ФЗ обязывают социальные сети, ежемесячная аудитория которых превышает 500 000 российских пользователей, регистрироваться в специальном реестре Роскомнадзора. После внесения в реестр площадка должна внедрить механизм оперативного удаления противоправного контента в течение 24 часов по требованию ведомства или по жалобам пользователей, а также вести отчетность о принятых мерах. Помимо классических экстремистских материалов под запрет подпадают призывы к участию в несогласованных митингах, распространение фейков о государственных институтах и пропаганда запрещенных товаров. Невыполнение этих обязанностей карается штрафами, достигающими 10 % годовой выручки, а в рецидивных случаях возможна замедление трафика или полная блокировка сервиса на территории РФ. На практике крупные платформы внедрили локальные офисы, автоматизированные фильтры и внутрироссийские представительские структуры для диалога с регулятором, тогда как некоторые зарубежные компании ограничили функции для российских пользователей или ушли с рынка, что отразилось на медийном ландшафте и уровне свободы выражения мнений.

2.6 Ответственность за нарушение законодательства

Российское ИТ-законодательство предусматривает многоуровневую систему санкций, которая варьируется от административных штрафов до уголовной ответственности, и применяется в зависимости от тяжести нарушения и наличия умысла. КоАП РФ содержит специализированные статьи, такие как 13.11 [9] (неправомерная обработка персональных данных) и 13.14 (раз-

глашение информации с ограниченным доступом), где максимальные административные штрафы для юридических лиц достигают 18 млн руб. за каждое эпизодическое нарушение . В уголовном кодексе предусмотрены статьи, которые квалифицируют незаконный доступ к компьютерной информации, создание вредоносных программ и нарушение правил эксплуатации средств хранения данных; наказание по ним варьируется от крупных штрафов и запрета занимать определенные должности до лишения свободы сроком до семи лет. Кроме того, в 2023 году введен механизм оборотных штрафов для крупных интернет-площадок, рассчитывающихся как процент от годового оборота, что стимулирует компании создавать комплексные программы комплаенса. На практике большинство дел завершается предписаниями и административными штрафами, но прецеденты возбуждения уголовных дел против должностных лиц демонстрируют серьезность подхода государства к защите цифрового суверенитета и персональных данных.

3 Юридические аспекты современных технологий

3.1 Защита интеллектуальной собственности

Правовая охрана результатов интеллектуальной деятельности в цифровой экономике строится на положениях четвертой части Гражданского кодекса РФ. Программное обеспечение признается объектом авторского права наравне с литературными произведениями, а это означает, что защита возникает автоматически с момента создания кода и не зависит от регистрации, хотя депонирование в Реестре программ может облегчить доказывание при споре. Для изобретений в области искусственного интеллекта и FinTech разработчики прибегают к патентованию технических решений, что обеспечивает более длительную монополию, но требует раскрытия сущности изобретения и прохождения экспертизы Роспатента. Международная составляющая регулирования обеспечивается применением Соглашения ТРИПС и участием России в Бернской конвенции, благодаря чему российские авторы получают охрану своих произведений за рубежом, а иностранные правообладатели - в России. На практике судебные споры все чаще касаются не классического копирования кода, а незаконного использования API, недобросовестного переноса модели данных или парсинга базы, поэтому суды ориентируются на совокупность доказательств, включая логи репозиториев, метаданные и экспертные заключения об оригинальности решений.

3.2 Электронная коммерция и онлайн-транзакции

Вопросы юридической силы операций в цифровой среде регламентируются Федеральным законом “Об электронной подписи” № 63-ФЗ [10] , который выделяет простую, усиленную неквалифицированную и усиленную квалифицированную подписи и связывает юридическую значимость документа с уровнем криптографической защиты и аккредитацией удостоверяющего центра. Права потребителей в интернет-магазинах защищаются Законом РФ “О защите прав потребителей” , обязывающим продавца раскрывать полную информацию о товаре, обеспечивать возможность возврата в течение семи дней и использовать понятные способы до- и постпродажного общения. Для расчетов применяются положения главы 45 ГК РФ о расчетных правоотношениях, но в трансграничном сегменте дополнительно действуют валютные и таможенные ограничения, а платежные сервисы должны соблюдать тре-

бования Росфинмониторинга по противодействию отмыванию средств. Развитие маркетплейсов стимулировало появление модели агентского договора с полной ответственностью платформы за качество доставки и возврата, однако суды по-прежнему разбирают вопросы о том, кто является продавцом при листинге товаров стороннего поставщика. В сфере цифровых активов ситуация остается фрагментированной: закон “О цифровых финансовых активах” признает токены объектами гражданских прав, но не предусматривает полноценного статуса для криптовалют, поэтому расчеты ими в электронной коммерции пока де-факто, а не де-юре.

3.3 Киберпреступность

Уголовный кодекс РФ содержит отдельную главу 28, к которой относятся статьи, предусматривающие ответственность за несанкционированный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, а также нарушение правил эксплуатации информационных систем . Превентивный акцент законодательства выражается в том, что состав преступления может быть окончен уже в момент попытки проникновения, даже если данных утекло незначительное количество. Поправки 2022 года расширили квалифицирующие признаки: к хищению теперь приравнивается массовый сбор учетных данных пользователей для последующей продажи на даркнет-площадках, а к тяжким последствиям - вывод из строя критической инфраструктуры. Государство усилило международное сотрудничество: Россия участвует в Шанхайской организации сотрудничества и в рамках ООН продвигает собственную конвенцию о противодействии киберпреступности, нацеливаясь на унификацию составов преступлений и быстрый обмен цифровыми доказательствами. На уровне правоприменения растет доля дел, возбужденных по материалам центров мониторинга трафика, а суды начинают принимать в качестве доказательств логи систем SIEM, данные ретроспективного анализа сетевых пакетов и заключения о цепочке блокчейн-транзакций.

4 Государственная поддержка IT-отрасли

4.1 Налоговые льготы для аккредитованных IT-компаний

Федеральный закон № 265-ФЗ от 31 июля 2020 года ввел специальный режим, который позволяет аккредитованным компаниям сократить совокупную налоговую нагрузку почти в три раза . Ставка страховых взносов вместо стандартных 30 % установлена на уровне 7,6 %, что высвобождает средства для найма разработчиков и R&D-проектах, особенно в регионах с высокой конкуренцией за кадры. Налог на прибыль уменьшен до 3 % в федеральный бюджет, а субъекты Федерации вправе установить нулевую ставку, чем уже воспользовались Татарстан и Нижегородская область, предлагая фактически беспрецедентный режим для центров разработки. Для операций по реализации ПО и оказанию услуг по разработке и поддержке действует освобождение от НДС, при условии что продукт включен в реестр российского ПО или услуги экспортируются, что делает российские облачные сервисы более конкурентоспособными за рубежом. Одновременно закон предусматривает жесткие критерии: доля профильных доходов должна превышать 70 %, среднесписочная численность - не менее семи сотрудников, а нарушения грозят возвратом недоимки и пеней за весь льготный период.

Таблица 4.1 - Налоговые льготы для аккредитованных IT-компаний

Льгота	Стандартная ставка	Льготная ставка
Социальное страхование	30%	7,6%
Налог на прибыль	20%	3% (федеральный), 0% (региональный)
НДС	20%	Освобождение для ПО и экспорта услуг

4.2 Государственное софинансирование цифровых проектов

Постановление Правительства № 1598 от 2 ноября 2019 года [11] определило правила отбора проектов, претендующих на субсидии на разработку и внедрение решений искусственного интеллекта и технологий обработки больших данных . Государство финансирует до 50 % расходов, а в приоритет-

ном списке - системы компьютерного зрения для промышленного контроля, интеллектуальные ассистенты для социальной сферы и платформы предиктивной аналитики в энергетике. Экспертный совет при Минцифры оценивает технологическую новизну, коммерческий потенциал и степень импортонезависимости, что стимулирует участников задействовать отечественные процессоры, базы данных и СУБД. Для получения средств заявитель должен предоставить дорожную карту, включающую KPI по выручке и количеству созданных высокопроизводительных рабочих мест, а освоение траншей контролируется казначейским сопровождением. С 2024 года параллельно запущена программа льготных займов ВЭБ.РФ под 1 % годовых для ИТ-проектов в сфере безопасности и GovTech, благодаря чему формируется комплексная система мер поддержки от идеи до промышленного внедрения.

5 Реализация IT-проектов в России

5.1 Процедуры и требования для IT-компаний

Организации-операторы персональных данных обязаны до начала обработки направить уведомление в Роскомнадзор по статье 22 Закона № 152-ФЗ, указав цели, категории субъектов, перечень обрабатываемых сведений и меры безопасности. Для банков, операторов связи и госпроектов дополнительно требуется построить систему защиты на базе национального стандарта ГОСТ Р 57580.1-2017, который описывает уровни зрелости, механизмы криптографической защиты и процедуры аудита . Комплексная проверка на соответствие стандарта проводится аккредитованными лабораториями, а результаты пересматриваются каждые три года или в случае значимых изменений архитектуры. Помимо этого, при создании госинформационной системы заказчик обязан пройти экспертизу ФСТЭК на соответствие приказу № 239, охватывающему контроль исходного кода, отсутствие недекларированных возможностей и устойчивость к нагрузочным атакам. В-целом путь от идеи до продуктивного запуска включает регистрацию прав на ПО, аккредитацию компании, сертификацию безопасности, постановку на налоговые льготы и, при наличии зарубежных пользователей, уведомление Роскомнадзора о трансграничной передаче данных.

5.2 Сотрудничество с иностранными партнерами

Договорная основа совместных ИТ-проектов с участием иностранных компаний формируется на базе главы 27 ГК РФ о купле-продаже и главы 39 о возмездном оказании услуг, а универсальным инструментом остается лицензионное соглашение. Чтобы контракт был исполнен в России, стороны включают оговорку о применимом праве и подсудности, а для хостинга персональных данных прописывают обязательство хранить зеркальную копию на территории РФ в соответствии со статьей 18 Закона № 152-ФЗ. При передаче исходного кода или технологии требуется получить заключение Минпромторга на предмет экспортного контроля, если продукт может иметь двойное назначение. В области облачных услуг выросла популярность схемы “technology partnership”, когда иностранный провайдер предоставляет платформу, а локальный оператор отвечает за комплаенс и взаимодействие с регуляторами; такая модель позволяет обойти прямые ограничения на владение критиче-

ской инфраструктурой иностранным лицом. На практике успешные проекты используют смешанную структуру: российская компания-интегратор несет ответственность перед госорганами, а иностранный разработчик поставляет обновления и SLA через сервисные соглашения, тем самым минимизируя риски, связанные с санкциями и валютным контролем.

6 Заключение

Законодательство России в сфере IT сочетает поддержку инноваций с жестким регулированием, основанным на теориях информационного права и кибербезопасности. Законы о Рунете, локализации данных и предустановке ПО стимулируют отечественную индустрию, но создают барьеры для иностранных компаний.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // 2006.

2. Постановление Правительства РФ № 1598 «О предоставлении субсидий на Искусственный интеллект и Big Data» // 2019.

3. Гражданский кодекс Российской Федерации, часть IV (ФЗ № 230-ФЗ) // 2006.

4. Федеральный закон № 152-ФЗ «О персональных данных» // 2006.

5. Федеральный закон № 38-ФЗ «О рекламе» // 2006.

6. Федеральный закон № 126-ФЗ «О связи» // 2003.

7. Федеральный закон № 90-ФЗ (суверенный интернет / «Закон о Рунете») // 2019.

8. Постановление Правительства РФ № 1236 «О приобретении российского программного обеспечения» // 2015.

9. Указ Президента РФ № 250 «О дополнительных мерах по обеспечению информационной безопасности» // 2022.

10. КоАП РФ, статья 13.11 «Неправомерная обработка персональных данных» // 2002.

11. Федеральный закон № 63-ФЗ «Об электронной подписи» // 2011.