Цифровые инструменты обеспечения финансовой безопасности

Правовое обеспечение информационной и кибербезопасности компаний: защита информационных активов (на примере Perimetrix SafeSpace)

Аннотация. *В условиях роста киберугроз, санкционных ограничений и усложнения цифровых цепочек взаимодействия защита информации ограниченного доступа становится не только технической, но и юридической задачей. В статье рассматриваются ключевые правовые режимы защиты информационных активов (коммерческая тайна, персональные данные, внутренняя конфиденциальная информация), требования к локальным актам и договорным конструкциям (NDA, условия о конфиденциальности, соглашения об обработке данных), а также виды юридической ответственности за нарушения режима конфиденциальности. Показано, что технические решения класса data-centric security и data classification могут выступать инструментом реализации правовых требований на практике, обеспечивая принцип «все запрещено, кроме явно разрешенного», разграничение доступа, шифрование, маркировку и сквозной аудит операций. В качестве прикладного кейса рассмотрен подход к построению комплаенс-контуров информационной безопасности на базе решения класса data-centric security (Perimetrix SafeSpace) и к снижению регуляторных и судебных рисков.*

Ключевые слова: *информация ограниченного доступа, режим конфиденциальности, коммерческая тайна, персональные данные, комплаенс, юридическая ответственность, информационная безопасность, кибербезопасность, Perimetrix SafeSpace*

DOI: 10.17803/2311-5998.2026.139.3.073-084

Антон Геннадьевич ЩЕРБАКОВ,
доцент аспирантуры Всероссийского научно-исследовательского института судостроительной промышленности «Центр», кандидат экономических наук
otadow@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 11, стр. 1

Алексей Александрович ТРИШИН,
исполнительный директор ООО «Периметрикс», аспирант базовой кафедры «Управление инновационной и промышленной политикой» Российского экономического университета имени Г. В. Плеханова
sro.trishin@mail.ru
123001, Россия, г. Москва, ул. Садовая-Кудринская, д. 8

Андрей Валерьевич ЖЕРЛИЦЫН,
коммерческий директор ООО «Развитие систем связи и энергетики»
info@rasst.ru
117218, Россия, г. Москва, ул. Кедрова, д. 14, корп. 2

Anton G. SHCHERBAKOV,
Associate Professor of Postgraduate studies
All-Russian Research Institute of Shipbuilding Industry «Center»,
Cand. Sci. (Economic)
otadow@gmail.com
11/1, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Alexey A. TRISHIN,
Executive Director,
LLC "Perimetrix",
Postgraduate student of the Basic department "Management of Innovation and Industrial Policy",
Plekhanov Russian University of Economics
sro.trishin@mail.ru
8, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 123001

Andrey V. ZHERLITSYN,
Commercial Director of Development of Communication and Energy Systems LLC
info@rasst.ru
14/2, ul. Kedrova, Moscow, Russia, 117218

Legal Support for Company Information and Cybersecurity: Protection of Information Assets (Case of Perimetrix SafeSpace)

Abstract. *In an environment of growing cyber threats, sanctions and complex digital supply chains, protection of restricted information becomes not only a technical but also a legal task. The article analyses key legal regimes for protecting information assets (trade secrets, personal data and internal confidential information), requirements for internal policies and contractual instruments (NDAs, confidentiality clauses, data processing agreements), and major forms of legal liability for confidentiality breaches. It is shown that data centric security and data classification solutions may serve as practical enforcement tools by implementing the "deny by default" principle, access control, encryption, labeling and end to end audit. Using Perimetrix SafeSpace as a case study, the paper outlines approaches to building an information security compliance framework and reducing regulatory and litigation risks.*
Keywords: *restricted information, confidentiality regime, trade secret, personal data, compliance, legal liability, information security, cybersecurity, Perimetrix SafeSpace*

1. Введение

Целью настоящего исследования является анализ правовых механизмов обеспечения защиты информационных активов организаций и выявление возможностей практической реализации требований законодательства посредством современных средств защиты данных. Для достижения поставленной цели решаются следующие задачи:

1) анализ правовых режимов информации ограниченного доступа;
2) исследование договорных и локальных инструментов обеспечения конфиденциальности;
3) оценка роли технических средств защиты данных в обеспечении правового комплаенса организаций.

Методологическую основу исследования составили формально-юридический, системный и сравнительно-правовой методы, а также анализ нормативных правовых актов и практики применения мер защиты информации в корпоративных информационных системах.

Цифровизация бизнес-процессов и рост объема обрабатываемых данных усилили зависимость компаний от сохранности информационных активов. Утечка либо компрометация данных приводят не только к прямым экономическим потерям и репутационному ущербу, но и к юридическим последствиям: претензиям контрагентов, мерам реагирования со стороны регуляторов, судебным спорам и привлечению к ответственности[1].

В условиях геополитических вызовов и технологических ограничений для российских организаций актуализируется задача выстраивания правомерного режима работы с информацией ограниченного доступа. Это предполагает сочетание организационных, договорных и технических мер, позволяющих подтвердить добросовестность и должную осмотрительность компании при защите информации.

2. Информационные активы и правовые режимы защиты

Информационный актив в корпоративном контуре — это любая информация, обладающая ценностью для организации (финансовые документы, клиентские базы, коммерческие предложения, результаты НИОКР, технологические инструкции, стратегические планы). В зависимости от правовой природы и способа легитимации режима доступа применяются различные правовые режимы. Основные категории информации ограниченного доступа и типовые меры организационной защиты представлены в табл. 1.

С практической точки зрения для большинства компаний ключевыми являются: 1) коммерческая тайна и иные сведения, охраняемые как секрет производства

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

(ноу-хау)[2]; 2) персональные данные[3]; 3) внутренняя конфиденциальная информация, режим которой устанавливается локальными актами и договорами[4]; 4) сведения, подпадающие под отраслевые требования (например, финансового сектора), а также информация, относимая к критической информационной инфраструктуре[5].

Таблица 1

Основные правовые режимы информации ограниченного доступа и типовые меры защиты

Категория информации	Правовой режим (пример источника)	Минимальные организационные меры (пример)
Коммерческая тайна (КТ), ноу-хау	Режим КТ / секрета производства (Закон «О коммерческой тайне», ГК РФ)	Перечень сведений; маркировка; допуск по принципу need-to-know; соглашение о конфиденциальности (NDA) / условия в договорах; учет носителей
Персональные данные (ПДн)	Режим ПДн (Закон «О персональных данных»)	Определение целей и оснований обработки; назначение ответственных; модель угроз и меры защиты; договоры с обработчиками; учет инцидентов
Внутренняя конфиденциальная информация	Локальные акты, договорные обязательства	Положение о конфиденциальности; разграничение прав; обучение; контроль вывода/передачи; дисциплинарные меры
Критическая ИТ-инфраструктура (при наличии)	Требования к безопасности критической информационной инфраструктуры (Закон «О безопасности критической информационной структуры РФ»)	Категорирование объектов; меры защиты и мониторинг; реагирование на инциденты; взаимодействие с регуляторами

3. Договорные и локальные инструменты обеспечения конфиденциальности

Юридическая составляющая информационной и кибербезопасности в компании во многом реализуется через внутренние документы и договорные

[2] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СПС «КонсультантПлюс».

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».

[4] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

[5] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

механизмы. К числу базовых локальных актов относятся: политика (положение) о конфиденциальной информации; регламент классификации и маркировки данных; порядок предоставления и отзыва доступа; инструкции по безопасной работе с данными; порядок расследования инцидентов и хранения доказательств (журналы, логи, отчеты)[6].

Договорные инструменты включают соглашения о неразглашении (NDA) с работниками и контрагентами, специальные условия о конфиденциальности в договорах подряда и оказания услуг, а также документы, регулирующие обработку персональных данных (в том числе поручение / соглашение с обработчиком и требования к мерам защиты). Важным элементом является закрепление ответственности сторон, порядка уведомления об инцидентах, аудита и возврата/уничтожения носителей информации[7].

4. Ответственность и правовые последствия утечек и инцидентов

Нарушение режима конфиденциальности может повлечь совокупность последствий: гражданско-правовые требования о возмещении убытков, взыскании неустоек и применении иных мер ответственности; административные санкции (в том числе за нарушения требований к защите отдельных категорий информации); трудовые последствия для работников (дисциплинарная ответственность и др.); а также уголовно-правовое преследование при наличии состава. Дополнительно возникают регуляторные последствия: предписания, проверки, ограничения на деятельность, требования к устранению нарушений.

Для минимизации юридических рисков критично документально подтверждать соблюдение режима конфиденциальности: наличие утвержденных политик, протоколов допуска, обучение, ведение технических журналов действий пользователей и администраторов, результатов аудитов. Именно связка «правила — контроль исполнения — доказательная база» позволяет компании обосновывать добросовестность и снижать вероятность негативных правовых последствий.

5. Технические меры как инструмент правового комплаенса

Правовые требования к защите информации, как правило, формулируются в виде обязанностей по обеспечению конфиденциальности, целостности и доступности, а также по ограничению доступа и фиксации действий пользователей. Их практическая реализация невозможна без технических средств контроля.

Ключевым подходом является принцип «все запрещено, за исключением явно разрешенного», близкий к концепциям наименьших привилегий и need-to-know. В контуре обработки информации ограниченного доступа это означает, что любые операции с данными (создание, хранение, копирование, пересылка, печать, перенос на внешние носители и т.д.) допускаются только в пределах явно

[6] Гражданский кодекс РФ // СПС «КонсультантПлюс».

[7] Трудовой кодекс РФ // СПС «КонсультантПлюс».

утвержденных политик. Такой подход снижает вероятность как внешних атак, так и внутренних инцидентов, связанных с человеческим фактором.

Теоретическая рамка — контроль доступа и управление потоками информации. В теории компьютерной безопасности контроль доступа традиционно описывается через дискретные (DAC), мандатные (MAC) и ролевые (RBAC) модели. Для режимов конфиденциальности принципиально важны мандатные подходы, где субъектам и объектам присваиваются метки безопасности, а допустимость операций определяется отношением доминирования (иерархией / «решеткой» уровней).

В корпоративной практике юридические требования затрагивают не только «вход» к данным, но и управление потоками информации: копирования, пересылки, выгрузки на внешние носители, печати, работы через веб-ресурсы и т.д. Поэтому комплаенс-контур должен уметь ограничивать именно перемещение данных между различными контекстами обработки и хранения.

Подход data-centric security реализует такую логику через классификацию (метки) и политики обращения с данными, а также через сквозной журнал событий. Это позволяет переводить нормы локальных актов и договоров о конфиденциальности в проверяемые правила и формировать доказательства их соблюдения[8].

6. Специальные программные средства защиты как инструмент юридически значимого контроля обращения с данными (на примере Perimetrix SafeSpace)

Практика показывает, что одних локальных актов, соглашений о конфиденциальности (NDA) и регламентов недостаточно для устойчивого режима защиты информации: в цифровой среде данные постоянно копируются, пересылаются, выводятся на печать и обрабатываются в десятках приложений и каналов. Поэтому для реализации юридических требований обычно применяются специальные средства защиты в виде программного обеспечения, которое делает правила исполнимыми (принцип «запрещено все, кроме явно разрешенного»), контролирует ключевые операции и формирует проверяемый аудит[9,10].

В качестве примера такого программного обеспечения далее рассматривается Perimetrix SafeSpace — решение класса data-centric security / data classification. Разработчиком является компания Perimetrix (российский разработчик

[8] ISO/IEC 27005:2022. Information technology — Security techniques — Information security risk management.

[9] *Грушо А. А., Применко Э. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности : учебное пособие для студентов вузов, обучающихся по специальностям группы 090100 «Информационная безопасность». М. : Академия, 2009.

[10] *Богульская Н. А., Кучеров М. М.* Модели безопасности компьютерных систем. Сибирский федеральный университет, 2019.

программного обеспечения, основана в 2007 г.), специализирующаяся на защите данных ограниченного доступа на всех этапах их жизненного цикла[11].

Далее показано, какую проблематику, поднятую в настоящей статье (идентификация режима, разграничение допусков, контроль передачи и доказательная база), можно «приземлить» в настройки подобных систем и почему без специализированного ПО эти задачи часто остаются преимущественно декларативными, так как сложно обеспечить единообразное применение правил на всех рабочих станциях, запретить несанкционированные перемещения и гарантировать полноту журналирования.

Ниже приведен практический разбор того, как требования по защите информации ограниченного доступа (коммерческая тайна, персональные данные, внутренняя конфиденциальная информация), описанные в разделах 2—4, могут быть переведены в исполнимые технические политики и процедуры контроля.

Важно подчеркнуть, что упоминание конкретного программного решения носит прикладной характер (case study). Цель — показать логику «норма/обязанность → контролируемая операция → журнал/доказательство», а не заменить юридический анализ описанием продукта или руководством пользователя.

6.1. Формализация требований: от локального акта к «матрице допустимых действий»

Юрист или комплаенс-функция обычно фиксирует правила в локальном акте (что считать конфиденциальным; кто и на каких основаниях имеет доступ; как можно передавать и хранить; какие действия запрещены; как вести учет и расследование). Для того чтобы правило стало исполнимым, его необходимо представить в виде перечня конкретных операций и условий их допустимости[12].

В решениях класса data-centric security эта формализация обычно опирается на два элемента: 1) метку / классификацию данных (уровень, проект, подразделение и др.) и 2) правила перемещения данных между контекстами обработки и хранения. В Perimetrix SafeSpace такой контекст задается «контейнером» (процесс, файл/папка, принтер, буфер обмена, сетевой ресурс, съемный носитель и т.п.), а действие описывается как перемещение из контейнера-источника в контейнер-приемник.

Практически это означает, что локальный акт о конфиденциальности целесообразно дополнять приложением-матрицей: «источник → куда можно → при каких условиях → что фиксируем». Такой формат облегчает как настройку технической политики, так и последующее доказывание соблюдения режима (проверки, споры, расследования).

[11] Perimetrix SafeSpace 2.8 : справочник по контейнерам. RU_PTX_SS28_CRG (версия 1.6.6).

[12] Perimetrix SafeSpace. Technical Prerequisites (v4.0, EN). Реестр программного обеспечения. Реестровая запись № 4120 от 11.12.2017 // URL: https://reestr.digital.gov.ru// (дата обращения: 20.03.2026).

6.2. Актуальные задачи, которые целесообразно «приземлять» в технические политики

С учетом рассмотренных правовых режимов и типовых рисков утечек для большинства организаций приоритетными являются следующие практические задачи:

— управляемая классификация и маркировка данных (чтобы режим был идентифицируемым и воспроизводимым: что именно защищаем и по каким правилам);
— разграничение доступа по принципу need-to-know и предотвращение обхода процедур через «сторонние» приложения или неучтенные хранилища;
— контроль ключевых каналов вывода/передачи: печать, буфер обмена, внешние носители, почта/мессенджеры, веб-формы, облачные сервисы;
— безопасное взаимодействие с контрагентами (обмен по NDA, возврат/уничтожение носителей, контроль передачи за периметр);
— контроль удаленного доступа к серверным и веб-ресурсам с конфиденциальной информацией (включая подтверждение «доверенности» клиента и фиксацию попыток доступа);
— формирование доказательственной базы (журналы действий пользователей и администраторов, фиксация конфигураций политик, отчетность для внутренних расследований и ответов регуляторам).

6.3. Как Perimetrix SafeSpace может поддержать выполнение задач

Практический смысл интеграции технического решения в юридический контур не в перечислении функций, а в том, чтобы каждая юридическая обязанность имела «точку контроля» и «след» в учетных данных (логах, отчетах, конфигурациях). Соотношение юридических задач защиты информации и технических механизмов их практической реализации может быть представлено в виде системы соответствия (табл. 2).

Таблица 2

Соответствие юридических задач и технических механизмов контроля (пример на базе Perimetrix SafeSpace)

Юридическая задача	Риск / типичный кейс нарушения	Механизм контроля (пример)	Доказательства / артефакты
Классификация и маркировка (КТ/ПДн/внутр.)	Смешение защищаемых и незащищаемых данных; невозможность доказать режим	Многомерные метки (уровень/проект/подразделение) + правила присвоения	Метки в свойствах объектов; журналы присвоения/изменения уровней
Ограничение доступа и «запрет по умолчанию»	Доступ «по привычке»; несанкционированное копирование/перемещение	Контейнеры + матрица разрешенных перемещений; блокировка неразрешенных операций	События разрешений/блокировок; актуальная конфигурация политики

Юридическая задача	Риск / типичный кейс нарушения	Механизм контроля (пример)	Доказательства / артефакты
Контроль каналов вывода и передачи	Вынос на флеш-носитель, отправка в облако/мессенджер, web-upload	Политики для буфера обмена, внешних носителей, веб-каналов и др.	Журналы событий по каналам; отчеты по нарушениям
Взаимодействие с контрагентами по NDA	Передача файлов «как есть» без контроля получателя и состава данных	Шифрованные контейнеры (Cryptex) и/или доверенные каналы передачи	События упаковки/передачи; параметры контейнера; перечень получателей
Удаленный доступ к серверным/веб-ресурсам	Доступ с недоверенных устройств; неконтролируемая загрузка/выгрузка	Контроль контекста доступа к ресурсам (SafeResource) + политики	Логи доступа, попыток, отказов; сведения о клиенте/контексте
Печать и бумажные копии	Неучтенные распечатки, подмена/фотокопирование без идентификации	Правила печати (SafePrint), учет, маркировка/идентификация копий	Журнал печати; параметры задания; идентификаторы/водяные знаки

Приведенные связки носят примерный характер. Конкретная конфигурация зависит от профиля организации, состава данных, каналов взаимодействия и требований локальных актов / договоров.

1. *Модель классификации (метки).* В SafeSpace поддерживается многомерная модель уровней, что позволяет увязать требования режима КТ/ПДн с внутренними признаками «проект/подразделение/территория» и реализовывать допуски по need-to-know.
2. *Контейнеры и правила перемещения.* Политики строятся вокруг допустимых перемещений данных между контейнерами. Это позволяет ограничивать не только доступ, но и вывод информации в «неконтролируемые» контексты (например, в личные папки, к облачным клиентам, во внешние носители).
3. *Доверенные приложения и режимы работы.* Закрепляя перечень допустимых процессов для работы с классифицированными данными и управляя режимами (классифицированный/неклассифицированный), можно снижать риск обхода режима через утилиты, не предназначенные для защищенной обработки.
4. *Контроль удаленных ресурсов и веб-порталов.* При наличии распределенной инфраструктуры юридически значимо контролировать, кто и с какого доверенного клиента обращается к защищенным ресурсам; в экосистеме Perimetrix это решается компонентом SafeResource, который проверяет контекст доступа и применяет политики.
5. *Управляемая передача во внешний периметр.* Для обмена с контрагентами может применяться шифрованный контейнер (Cryptex) с контролем

уровней и фиксацией событий упаковки/передачи — это помогает выполнять требования NDA и управлять рисками «утечки по каналу передачи».

6. *Контроль печати и бумажных копий.* Компонент SafePrint позволяет вводить правила печати (разрешения, учет, маркировку/идентификацию) и тем самым закрывать один из типовых каналов несанкционированного распространения.
7. *Инвентаризация и доведение режима до «сплошного».* На практике существенная часть рисков связана с «серой зоной» — файлами без классификации и вне регламентированных хранилищ. Инструменты инвентаризации (DataSure) позволяют выявлять такие массивы для последующей правомерной классификации и переноса в доверенные контуры.

6.4. Пример сквозного сценария: коммерческая тайна + подрядчик

Если компания вводит режим коммерческой тайны по группе документов «договоры/цены/технологии» и привлекает подрядчика (например, на проектные или ИТ-работы), задача юриста — обеспечить исполнимость условий NDA и управляемость передачи материалов. Технически это может быть реализовано через: классификацию документов; хранение в доверенных сетевых папках; разрешение работы только в доверенных приложениях; запрет вывода в неконтролируемые каналы (облака /внешние носители /неучтенные почтовые клиенты); передачу подрядчику через шифрованный контейнер (Cryptex) с контролем уровней; а также фиксацию событий передачи в журналах для последующего аудита.

При таком подходе Perimetrix используется как «исполнитель» заранее сформулированных юридических правил: система не подменяет локальные акты и договорные обязанности, но помогает обеспечить их соблюдение за счет контроля операций с данными и фиксации событий.

6.5. Аудит и доказательства: что предусмотреть заранее

Чтобы технический контроль реально снижал правовые риски, вопросы доказательств нужно закладывать в проект внедрения: сроки и порядок хранения журналов; перечень ответственных; регламент выгрузки логов и фиксации версий политик; правила внутреннего расследования и уведомления (для ПДн и договорных обязательств).

Практически полезно заранее определить набор артефактов, которые компания сможет предъявить: действующие локальные акты и NDA; матрицу допусков; конфигурации политик; журналы разрешенных и заблокированных операций; отчеты по инцидентам и корректирующим мерам. Связка «правило — контроль — доказательство» делает режим конфиденциальности проверяемым и защищает организацию в спорных ситуациях.

6.6. Правовое оформление технических механизмов защиты информации

Внедрение технических средств защиты данных само по себе не обеспечивает юридической значимости режима конфиденциальности. Для того чтобы контроль операций с информацией мог рассматриваться как элемент правомерного режима

защиты информации, соответствующие механизмы должны быть закреплены в системе локальных нормативных актов организации.

К числу таких актов могут относиться: положение о конфиденциальной информации и коммерческой тайне; политика классификации и маркировки данных; регламент управления доступом к информационным ресурсам; порядок использования съемных носителей и внешних каналов передачи данных; регламент взаимодействия с контрагентами при передаче конфиденциальной информации; порядок расследования инцидентов информационной безопасности.

В указанных документах целесообразно закреплять правила обращения с информацией ограниченного доступа, включая порядок ее классификации, перечень допустимых операций с данными, правила передачи информации за пределы организации, а также процедуры аудита и фиксации действий пользователей.

Технические средства защиты информации, включая системы класса data-centric security, в таком случае выступают инструментом реализации закрепленных правовых требований и позволяют обеспечить контроль их исполнения. Наличие журналов операций, конфигураций политик и отчетности по инцидентам формирует доказательственную базу, которая может использоваться при внутренних расследованиях, проверках регуляторов и судебных разбирательствах.

7. Заключение

Информационная и кибербезопасность компаний в современной экономике выступают предметом не только технического управления, но и правового комплаенса. Эффективная защита информационных активов требует построения юридически корректного режима конфиденциальности (локальные акты и договоры), определения ответственности и процедур реагирования, а также внедрения технических средств, обеспечивающих контроль исполнения правил.

Пример внедрения решения класса data-centric security (Perimetrix SafeSpace) демонстрирует, что принцип «запрещено все, кроме явно разрешенного», реализованный через классификацию данных и аудит операций, может служить практическим механизмом исполнения требований локальных актов и договоров о конфиденциальности, а также снижать регуляторные и судебные риски при инцидентах.

Проведенный анализ показывает, что современная система защиты информационных активов компаний должна рассматриваться как комплексная правовая и организационно-техническая конструкция. Наличие формально закрепленных режимов конфиденциальности, договорных обязательств и локальных нормативных актов создает правовую основу защиты информации, тогда как технические средства обеспечивают исполнимость соответствующих требований на практике.

Использование систем класса data-centric security позволяет реализовать принципы минимально необходимого доступа, контролируемого перемещения данных и сквозного аудита операций, что повышает уровень корпоративного комплаенса и снижает регуляторные и судебные риски при инцидентах информационной безопасности.

Таким образом, эффективная защита информационных активов требует интеграции правовых механизмов регулирования и современных технологий контроля обращения с данными.

БИБЛИОГРАФИЯ

1. *Бачило И. Л.* Информационное право : учебник для вузов / И. Л. Бачило. — 5-е изд., перераб. и доп. — М. : Юрайт, 2026. — 419 с.
2. *Богульская Н. А., Кучеров М. М.* Модели безопасности компьютерных систем. — Сибирский федеральный университет, 2019. — 206 с.
3. *Грушо А. А., Применко Э. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности : учебное пособие для студентов вузов, обучающихся по специальностям группы 090100 «Информационная безопасность». — М. : Академия, 2009. — 267 с.
4. *Малько А. В., Костенко М. А.* Место и роль юридических технологий в правотворческой политике современной России // Журнал российского права. — 2017. — № 4. — С. 5—15.
5. *Поляков А. В.* Правовые основы информационной безопасности. — Воронеж : Научная книга, 2021. — 80 с.
6. *Талапина Э. В.* Право и цифровизация: новые вызовы и перспективы // Журнал российского права. — 2018. — № 2. — С. 5—17.