СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ: ПРИНЦИПЫ, КЛАССИФИКАЦИЯ, МЕТОДЫ И ТЕХНОЛОГИИ

Минзов А. С.[1], Невский А. Ю.[2], Минзов С. А.[3]

DOI: 10.21681/2311-3456-2025-5-2-14

Цель исследования: *обоснование системы защиты коммерческой тайны в различных формах ее представления на основе классификации, обоснования принципов, методов и технологий защиты.*

Методы исследования: *ретроспективный анализ требований к защите коммерческой тайны в России и за рубежом, системный анализ при обосновании классификации коммерческой тайны, концептуальное моделирование системы её защиты на основе концепции «нулевого доверия» (Zero Trust), синтез системы защиты коммерческой тайны на всех этапах её жизненного цикла.*

Результаты исследования: *полученные результаты не противоречат существующим нормативным документам по защите коммерческой тайны и могут быть использованы для усиления защитных свойств различных объектов, где возникает необходимость защиты коммерческой тайны в России и за рубежом.*

Научная новизна: *в статье предложены новые подходы к классификации коммерческой тайны с позиций её защиты от разглашения (утечки), принципы защиты коммерческой тайны на основе концепции «нулевого доверия» и система управления защитой коммерческой тайны в виде циклического управляемого защищаемого процесса от создания инновационной идеи, проектирования, внедрения и её эксплуатации.*

Практическая значимость: *предложенные авторами решения и подходы к защите коммерческой тайны позволят повысить уровень защищенности хозяйствующих субъектов, где возникает необходимость её защиты, увеличить инновационную активность в рыночных отношениях и противодействовать промышленному и экономическому шпионажу.*

Ключевые слова: *trade secret, система защиты информации, режим коммерческой тайны, zero trust, нулевое доверие.*

Введение

Понятие «коммерческая тайна» (*trade secret*) впервые появилось в странах с рыночной экономикой в середине 18-го века и законодательно оформлена в современной трактовке в США и европейских странах только в конце 20-го века. Многие исследователи связывают интенсивный экономический рост европейских государств и США с созданием правового института защиты коммерческой тайны [1]. Современное представление о коммерческой тайне во многом основано на принятом в США в 1979 г. законе «О коммерческой тайне» (Uniform Trade Secret Act) [2]. В этом законе коммерческая тайна (КТ) определяется как «***информация*** (включая формулы, модели, программы, механизмы, способы, технологии) или ***технология***, обладающая самостоятельной экономической ценностью (действительной или потенциальной) и недоступна для других лиц, которые могли бы извлечь экономическую выгоду из ее использования или разглашения, и в отношении которой приняты меры по защите ее секретности» [3]. В этом определении есть некоторые противоречия, связанные с классификацией КТ. Например, что включает в себя информационная технология, если в понятие «информация» включены программы и модели? О каких технологиях идет речь в классе «технологии»? Почему данные (маркетинговые, социологические и другие исследования) не могут быть отнесены к КТ в определении КТ?

Эти и другие вопросы не позволяют в судебной практике США четко определить отношения объекта права к КТ. Поэтому было разработано дополнение и определены вопросы, по которым необходимо провести исследование для определения возможного отнесения объекта права к КТ и обоснования судебных решений по КТ, которое включает [4,5]:

1. Экономическую ценность информации для владельца КТ и его конкурентов.
2. Степень известности информации о КТ за пределами бизнеса, использующего КТ.
3. Степень известности этой информации сотрудникам и другим лицам, участвующим в этом бизнесе.
4. Уровень мер, принимаемых владельцем бизнеса по охране конфиденциальности информации о КТ.

1 Минзов Анатолий Степанович, доктор технических наук, профессор, Национальный исследовательский университет МЭИ, г. Москва, Россия. E-mail: MinzovAS@mpei.ru

2 Невский Александр Юрьевич, кандидат технических наук, доцент, Национальный исследовательский университет МЭИ, г. Москва, Россия. E-mail: NevskiyAY@mpei.ru

3 Минзов Степан Анатольевич, заместитель начальника отдела АСУ(БД) АКБ «Фора-Банк», г. Москва, Россия. E-mail: minzov@forabank.ru

5. Количество усилий или средств, затраченных на разработку КТ.
6. Легкость или сложность, с которой информация может быть надлежащим образом получена или воспроизведена другими.

К сожалению, значение критериев для этих вопросов не были конкретно определены, поэтому при решении задач защиты КТ в судах США возникают проблемы отнесения объекта права к КТ. И, тем не менее, приведенное выше определение КТ и классификация вопросов, по которым принимается судебное решение, имеет весьма глубокий смысл, который в современном представлении включает в себя условия, требования и механизмы защиты КТ. Сформулируем эти условия с точки зрения защиты информации.

Первым условием отнесения информации к КТ является ее экономическая ценность. Это означает, что владелец тайны должен уметь *доказать (продемонстрировать) её экономическую эффективность (выгоду)*. Из этого следует, что коммерческая тайна будет защищаться государством до тех пор, пока её владелец сможет доказать её экономическую ценность. Это очень важный момент прекращения действия режима защиты КТ со стороны государства. Отсюда вывод: если КТ не имеет экономической ценности, то нет смысла ее защищать.

Второе условие заключается в том, что КТ должна быть недоступна для лиц за пределами бизнеса, которые могут её использовать. Здесь следует отметить, что любая тайна создается не мгновенно, а путём интеллектуальной целенаправленной деятельности её владельца. Отсюда возникает необходимость защиты КТ на всех этапах её проектирования и внедрения, а не только на этапе её применения. Очень важное следствие из анализа этого условия заключается в том, что КТ основывается на инновационных решениях, которые могут принести экономическую выгоду. Современная методология создания инновационных проектов предусматривает набор процессов от генерации инновационных идей, до разработки инновационного проекта, его внедрения и создания механизмов его защиты. Следовательно, все эти процессы должны быть защищены.

Третье условие заключается в создании таких требований к разработке КТ, ее внедрению и эксплуатации, при которых распространение КТ среди персонала организации является *минимально необходимым и контролируемым*. Следует отметить, что такая форма интерпретации этого условия с позиций защиты КТ в зарубежной печати отсутствует.

Четвертое условие заключается в обеспечении владельцем КТ разумных и достаточных мер её защиты. Критерии «разумности» и достаточности» защиты в законодательства США и Европы четко не определены и, обычно, выясняются судом присяжных в судебном процессе путем оценки разумности мероприятий при организации защиты КТ. Следует отметить, что выполнение этого условия практически не регулируется и носит общий характер, который можно сформулировать в форме следующих рекомендаций [5]:

1) предупреждение сотрудников и третьих сторон о конфиденциальном характере информации посредством соглашений о конфиденциальности, указаний на конфиденциальность в документах;
2) реализация программ профессиональной подготовки для сотрудников или в инструкциях по работе с КТ для сотрудников;
3) защита паролей и межсетевых экранов;
4) физическая блокировка конфиденциальной информации;
5) ограничение доступа к физическим и электронным архивам, где хранятся коммерческие секреты;
6) минимизация количества сотрудников, допущенных к КТ.

При этом, совершенно открытым остается вопрос: а этих мер достаточно для защиты КТ?

Пятое условие связано с первым и используется для оценки значимости КТ. Оно используется для того, чтобы можно было обосновать некоторую модель ответственности[4] за разглашение КТ. Кроме того, этот фактор связан с экономической ценностью КТ для определения максимального размера разумных затрат на систему защиты КТ.

Шестое условие, так же, как и пятое, связано непосредственно с моделью ответственности за разглашение (утечку) информации как со стороны владельца коммерческой тайны, так и со стороны сотрудника, который её разгласил. С учетом увеличивающейся ценности коммерческих секретов и сложности их защиты в США в 1996 г. был принят Акт об экономическом шпионаже, согласно которому кража коммерческих секретов приравнена к федеральному уголовному преступлению, с административным наказанием в виде штрафа до 10 млн долл. США и уголовным сроком до 15 лет [3].

В зарубежных научных обзорах рассматриваются вопросы разработки параллельных проектов КТ в разных организациях. С точки зрения зарубежного законодательства считается вполне допустимым, если результаты достигаются с использованием различных технологий, материалов, методов, условий и других факторов. Такое отношение к параллельным

4 Под термином «модель ответственности» мы понимаем условия, при которых либо применяется законодательство с обоснованием определенных мер ответственности за разглашение (утечку) КТ, либо не применяется законодательство при невыполнении условий защиты или отсутствии доказательства разглашения или утечки КТ.

проектам КТ вполне логично. В мире известно много параллельных научных достижений, выполненных разными учеными в одно время. Например, Александр Попов и Гульельмо Маркони – изобретатели радио, Дмитрий Менделеев и Лотар Мейер создатели периодической системы элементов, позволяющей предсказывать наличие новых элементов в этой системе и другие подобные примеры. Такие коллизии могут быть следствием параллельной разработки известных проблем из открытых источников. Это подтверждает наш тезис о том, что КТ должна защищаться на этапе постановки задачи проекта, относящегося к КТ.

Не менее важным для обсуждения остается вопрос отношений КТ, патента и полезной модели. Патент и коммерческая тайна (ноу-хау) – это два разных способа защиты интеллектуальной собственности, но у них есть и общие черты. Патент предоставляет исключительные права на изобретение на определенный срок (обычно 20 лет), в обмен на публичное раскрытие информации о нем и охраняется государством. Информация о патенте приводится на уровне понимания его сущности, с приведением технического её описания и доказательства новизны. КТ, напротив, предполагает сохранение этой информации в тайне, и ее защита может длиться неограниченно долго, пока информация остается секретной. Есть разница и между понятиями ноу-хау и КТ. КТ – это более общее понятие и главное ее свойство – это секрет, который дает преимущество в рыночных отношениях, а термин ноу-хау относится к тайне производства, которая также имеет экономическую ценность.

Анализ вопросов защиты коммерческой тайны был бы неполным, если бы не были рассмотрены законодательства КТ в других странах. Среди них наиболее интересными в области защиты КТ является законодательства Китая и Японии.

В КНР защита КТ регулируется законом о противодействии недобросовестной конкуренции (Anti-Unfair Competition Law [6]). Этот закон во многом повторяет законодательство США, также определяет коммерческую тайну, устанавливает требования к владельцам КТ и правила ее защиты. Основные требования к владельцам коммерческой тайны в КНР можно сформулировать в следующем виде:

1. Доказательство статуса коммерческой тайны:
   a) Информация должна быть секретной и не общедоступной.
   b) Информация должна иметь экономическую ценность.
   c) Владельцы должны принимать разумные меры для защиты этой информации.
2. Меры по защите КТ:
   a) Владельцы должны внедрять внутренние процедуры и политику для защиты информации, такие как соглашения о конфиденциальности и ограничение доступа.
3. Доказательства утечки КТ:
   a) Владельцы должны иметь возможность продемонстрировать (доказать), как и кем была разглашена КТ.

Очевидно, что существенным различием этих требований с законодательством США в сфере КТ является требование к владельцу КТ по созданию системы контроля использования КТ и *определения источника ее разглашения*. Это требование создает повышенные сложности в создании системы защиты КТ для ее владельцев.

Защита коммерческой тайны Японии регулируется законом о предотвращении утечки коммерческой тайны (Act on the Prevention of Unauthorized Use of a Trade Secret [7]) и практически не отличается от требований сформулированных в законодательстве КНР.

В заключение этого раздела анализа концепции защиты коммерческой тайны в зарубежном законодательстве остановимся на следующих особенностях:

1. Практически во всех законодательных актах зарубежных государств коммерческая тайна рассматривается как очень важная инновационная деятельность (Ноу-хау), направленная на развитие экономического, технологического, производственного и научного суверенитета государства в рыночных отношениях. Несовершенство законодательных актов в сфере защиты КТ приводит к повышению уровня промышленного шпионажа и недобросовестной конкуренции, усложняет проведение расследований преступлений по разглашению КТ и замедляет развитие экономической деятельности хозяйствующих субъектов.
2. Следует отметить, что в настоящее время не существует совершенного законодательства по защите КТ и это связано с различными формами её представления и классификациями, неопределёнными критериями «разумности и достаточности» её защиты, требованиями по предоставлению системы доказательств разглашения (утечки) информации. Это усложняет процедуры защиты КТ в судах.
3. Слабые стороны режимов защиты коммерческой тайны предприятий, которые обеспечивают очень узкий набор требований к защитным мерам КТ и не гарантируют доверия к системе ее защиты. Это являются одной из основных проблем в области управления коммерческой тайной.

4. Весьма поверхностно проработаны вопросы применения систем искусственного интеллекта при проектировании КТ (модели GPT, промпты, Data-Sets и результаты решения задач). Как в этом случае идентифицировать утечку КТ ?

Состояние вопроса по рассматриваемой проблеме в России

В Российской империи в начале 20 века юрист В. В. Розенберг предложил ввести термин «промысловая тайна», однако, этот термин не прижился и вместо него окончательно утвердился термин «коммерческая тайна», объединяющий тайну любой деятельности, имеющей целью извлечение прибыли [8].

После победы Великой Октябрьской социалистической революции уже 27 ноября 1917 г. положением о рабочем контроле, принятым ВЦИК и СНК РСФСР коммерческая тайна была упразднена. В 30-х годах институт коммерческой тайны был заменен государственной и военной тайной. Инновационная деятельность населения в этот период времени поощрялась в форме рационализаторских предложений, трудовых движений, рекордов и других форм инновационной активности населения. Но главное, результаты этой деятельности свободно распространялись в стране. На наш взгляд, именно такая форма инновационной деятельности общества сыграла значительную роль в экономическом развитии СССР в период 20-х – 40-х годов прошлого столетия.

Возрождение во второй половине 80-х гг. предпринимательской деятельности и переход страны к рыночным отношениям повлекли за собой разработку нормативных документов, в том числе касающихся коммерческой тайны. В первую очередь потребовалось сформулировать определение коммерческой тайны. Такое определение было дано в Законе СССР «О предприятиях в СССР» от 4 июня 1990 г. В нем сказано: «Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам». Руководителю предприятия предоставлялось право определять состав, объем и порядок защиты сведений, составляющих коммерческую тайну.

В отечественном законодательстве учитывается опыт зарубежных правовых механизмов защиты коммерческой тайны. Тем не менее, развитие системы защиты КТ в нашей стране имеет свои особенности, главная из которых заключается в несколько упрощенной форме её защиты путем создания только режима конфиденциальности (ограничения доступа) к коммерческой тайне, что обеспечивается созданием механизма ответственности за ее разглашение и ряда других организационных мер. Такой подход был заимствован из зарубежных законодательных актов и, как нами было рассмотрено ранее, является поверхностным по отношению к защите КТ. Современные условия требуют более совершенных механизмов защиты КТ особенно, если это касается торговых отношений с другими государствами. На международной конференции по комплексной защите информации было высказано мнение о том, что «ущерб от разглашения коммерческой тайны часто выше, чем от разглашения государственной тайны, как бы кощунственно это не звучало[5]».

Сегодня остаются открытыми несколько вопросов, в том числе: достаточно ли этих мер для защиты КТ, необходимо ли усиливать роль государства в защите КТ, обеспечивает ли режим защиту от недобросовестной конкуренции и другие. Все это требует научного анализа построения системы защиты КТ для различных условий и форм ее представления.

Но начнем анализ с определения понятия «коммерческая тайна» в отечественном законодательстве. В настоящее время защита КТ определяется Федеральным законом № 98[6]. В этом документе коммерческая тайна рассматривается как «*сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны*».

Столь сложная трактовка этого определения, по существу, относит к коммерческой тайне любую деятельность за исключением сведений, рассматриваемых в статье № 5 Федерально закона «О коммерческой тайне», не относящиеся к другим видам тайн и в других ФЗ, определяющих сведения, доступные для всех. На наш взгляд, в этом законе не могут присутствовать слова с неопределённым смыслом, такие как, «*и другие*», «*действительная или потенциальная коммерческая ценность*». Есть и нарушения логики, когда коммерческая тайна определяются сначала как «сведения любого характера» и приводятся примеры этой тайны, а затем следует фраза «*и другие*» (сведения), что требует уточнения формулировки понятия «коммерческая тайна», а также введение четкой классификации видов и форм её представления. Это вполне очевидно, так как невозможно

5 Рособоронэкспорт озаботился защитой информации / 7-я Международная конференция «Комплексная защита информации», 25–27 февраля 2025 г. Минск. URL: https://www.cnews.ru/articles/rosoboroneksport_ozabotilsya_zashchitoj (дата обращения: 01.09.2025).

6 ФЗ №98 «О коммерческой тайне», 2006 г.

построить одинаковую защиту информации, если она представлена в разных формах. Например, защищенный бумажный документооборот отличается от электронного документооборота и способы защиты информации совершенно отличаются друг от друга.

В составе коммерческой тайны некоторые специалисты выделяют две категории сведений: информация являющаяся результатом интеллектуальной деятельности и другие сведения, которые также относятся к коммерческой тайне [9]. Вторая категория коммерческой тайны является весьма субъективной и может представлять собой регистры внутреннего бухгалтерского учёта, досье на конкурентов, списки клиентов, результаты деловой разведки и другую подобную информацию. Определить экономическую ценность этой информации практически невозможно. Точно также невозможно и определить степень ущерба, который может быть нанесён организации, если эта информация получит огласку. Надо ли в этом случае вводить эту информацию в статус коммерческой тайны и привлекать государственные институты для решения проблем с ответственностью при её разглашении или утечке? Этот вопрос для нас остается открытым. Зарубежное законодательство сфокусировано на первой категории КТ.

Защита КТ по ФЗ № 98 осуществляется путем создания и введения правового режима коммерческой тайны в организации, который включает:

- ограничение доступа к информации;
- обозначение носителей информации грифом «Коммерческая тайна»;
- ознакомление работников с правилами обращения с конфиденциальной информацией;
- заключение с работниками соглашений о неразглашении;
- определение ответственных лиц за соблюдение режима коммерческой тайны.

Следует отметить, что этих мер во многих случаях недостаточно и требуется уточнение необходимых мер для различных форм представления КТ. Требования к обладателям КТ в этом ФЗ конкретно не определены в части: разумности и достаточности принятых ими защитных мер, возможности предоставления доказательств об экономической ценности КТ и о каналах утечки данных (разглашении) о КТ.

Более полную ясность в понятие «коммерческая тайна» вносит методический документ[7]. В нём под коммерческой тайной понимается режим конфиденциальности информации (ограничения доступа), позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Здесь требуется сделать отступление и вернуться к понятию «коммерция». Этот термин в современном представлении имеет более широкий смысл, чем это было несколько десятков лет тому назад. Коммерция (от лат. commercium – торговля, купля), предпринимательская деятельность экономических агентов – государства, компаний, домохозяйств, нацеленная на получение прибыли (производство товаров, оказание платных услуг, проведение обменных операций, осуществление инвестиций на финансовых рынках и т. д.); в узком смысле – это торговля[8]. Есть ещё одна интересная деталь. На западе и в США коммерческая тайна рассматривается как ***Trade Secret*** [2], что имеет смысл как «секрет рыночных отношений». В такой формулировке вложен более глубокий смысл, чем термин «коммерческая тайна». На наш взгляд, более точное понимание смысла коммерческой тайны заключается в том, что ***это результат интеллектуальной деятельности человека или системы искусственного интеллекта, направленный на совершенствование товаров или услуг в системе рыночных отношений и получения экономической выгоды***. Использование искусственного интеллекта для решения инновационных задач с одной стороны позволяет расширить возможности субъектов рыночных отношений в совершенствовании товаров и услуг, а с другой стороны вызывает необходимость усиленной защиты систем искусственного интеллекта и результатов их деятельности.

Решение ***первой задачи*** может быть основано на методах генеративного искусственного интеллекта [10–13] или путем поиска решений на основе технологий творческого проектирования (Метод А. Половинкина) [14] и теории решения изобретательских задач (ТРИЗ) [15].

Вторая задача связана с новым направлениям кибербезопасности систем искусственного интеллекта и обеспечения защиты от угроз [16–18]. Однозначного решения защиты систем искусственного интеллекта, генерирующего инновационные решения, относящиеся к коммерческой тайне от угроз сегодня не существует.

По мнению авторов статьи [19] искусственный интеллект поднимает множество и других сложных вопросов для законодательства:

- Защита технологий ИИ как коммерческой тайны.
- Защита результатов работы систем ИИ как коммерческой тайны.

7 Разъяснение Президиума ФАС России от 21.02.2018 N 13 «Об информации, составляющей коммерческую тайну, в рамках рассмотрения дела о нарушении антимонопольного законодательства, проведении проверок соблюдения антимонопольного законодательства, осуществлении государственного контроля за экономической концентрацией» (утв. протоколом Президиума ФАС России от 21.02.2018 N 2).

8 Большая Российская энциклопедия, 2022 г.

- Риски для коммерческой тайны, когда модель генеративного ИИ не может дать точного ответа и дает искажённый результат (bias) или галлюцинирует [20].
- Определение разницы между ИИ с закрытым и открытым исходным кодом и оценка их последствий для коммерческой тайны.

На наш взгляд, защите КТ с использованием ИИ также должны подвергаться и сценарии работы с ChatGPT (prompt и pipeline), которые и определяют результаты работы ИИ.

Очень важно, что современное понятие «коммерческая тайна» распространяется на широкий круг субъектов торговых отношений. Среди них сегодня выделяется крупные компании и государственные корпорации такие как РосАтом, Газпром, Роснефть, ОАО «ФСК ЕЭС», Рособоронэкспорт, а также НИИ, ВУЗы, многие производственные и другие организации. Практически во всем мире сложилась ситуация, когда каждое государство не только выполняет свои обязательства по защите коммерческой тайны, но и обеспечивает развитие научно-технического потенциала субъектов рыночных отношений за счёт выполнения ими инновационных проектов, относящихся к коммерческой тайне и имеющих преимущество на рынке товаров и услуг. К сожалению, эта сторона коммерческой тайны, как направление управления развитием научно-технического и технологического потенциала страны, в нашей научной среде сегодня практически не обсуждается, хотя такая потребность существует. Этот тезис подтверждается и в зарубежных исследованиях [1], но даже в тех странах, где коммерческая тайна защищается государством более 200 лет (США и европейские страны) вопрос ставится только об изучении влияния коммерческой тайны на развитие инновационного потенциала. Вопросы управления этим потенциалом не рассматриваются.

Таким образом, создание только режима защиты коммерческой тайны по Российскому законодательства в условиях применение систем ИИ для нахождения инновационных решений в системе рыночных отношений явно недостаточно.

Утверждение этого тезиса мы находим и в других зарубежных аналитических исследованиях по проблемам коммерческой тайны: «слабые стороны режимов защиты коммерческой тайны предприятий, низкий уровень деловой осведомленности, ограничение мобильности сотрудников, кибербезопасность, слабые стороны идентификации и защиты коммерческой тайны являются одними из основных политических проблем в области управления коммерческой тайной сегодня» [4].

Концепция и принципы защиты коммерческой тайны

Существующая концепция защиты коммерческой тайны сегодня определена Федеральным законом № 98 и заключается в создании правового режима коммерческой тайны. Мы уже отмечали ранее, что этот режим не обеспечивает достаточную защиту коммерческой тайны и требует совершенствования. Возникает вопрос, а что в этом случае можно применить? Сегодня в РФ существует ряд нормативно-методических документов в форме постановлений Правительства РФ, приказов ФСТЭК и методических документов[9], определяющих требования по защите конфиденциальной информации, относящиеся к персональным данным, государственным учреждениям, банковской тайне и значимым объектом критической информационной инфраструктуры. Для информации, не относящиеся к конфиденциальной, применяются государственные стандарты серии ГОСТ Р ИСО/МЭК 27000, которые являются эквивалентами международных стандартов ISO/IEC 27000. Концепции защиты информации в этих двух группах нормативно-методических документов, действующих на территории РФ, существенно отличаются. Если группа отечественных нормативно-методических документов меры по защите информации определяет в зависимости от класса или уровня защищенности информационной системы, то группа международных стандартов рекомендует использовать меры в зависимости от уровня рисков безопасности информации. Оценка возможности применения этих концепций защиты коммерческой тайны показывает, что ни одна из них не может быть использована в полной мере. Основная причина заключается в том, что система защиты КТ *работает только до первой реализации угрозы утечки (разглашения) КТ*. После этого нет необходимости в ее защите, так как дальнейшее ее применение уже не даст экономических выгод и, следовательно, не целесообразно. Это требует другой концепции создания архитектуры информационной безопасности, основанной на более высоком уровне защищенности КТ и доверия к ней.

Как в настоящее время создаются системы с заданным, повышенным или измеряемым уровнями доверия к ним?

Доверие к ИТ-проектам в концепции стандарта ГОСТ 15408[10] это «основа для уверенности в том, что продукт ИТ отвечает целям безопасности».

В этом стандарте определен и механизм обеспечения доверия к системе информационной безопасности, как «бездоказательное утверждение,

9 Вся система нормативно-методических документов приведена сайте ФСТЭК https://fstec.ru.

10 ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

предшествующий аналогичный или специфический опыт», а также с использованием активного исследования ИТ-продукта для определения его свойств безопасности. Требования доверия представляются в виде структуры: класс–семейство–компонент–элемент. Основные принципы этого стандарта состоят в том, что следует четко сформулировать угрозы безопасности, положения политики безопасности организации и продемонстрировать достаточность предложенных мер безопасности.

Основной способ достижения доверия к системе информационной безопасности основан на проведении его оценки (всего 6 уровней оценки доверия[11]). Методы оценки основаны на анализе процессов, требований к ним, верификации доказательств, независимом функциональном тестировании, анализе уязвимостей и тестировании на проникновение.

Доверие к техническим средствам ИТ-проектов обеспечивается транзитивно путем применения сертифицированных технических средств, удостоверяющих центров и других средств, имеющих сертификаты соответствия. Кроме того, доверие к системе информационной безопасности может быть обеспечено и другими средствами, методами и технологиями:

1. Аттестацией объектов информатизации.
2. Оценкой соответствия требований к системе управления ИБ через её аудит (ГОСТ Р ИСО/МЭК 27002-21 г.).
3. Применением абстрактных формальных моделей доступа, целостности и доступности (Модель Белла–ЛаПадулы, Биба, Clark–Wilson, Take–Grant и др.).
4. Тестированием системы ИБ на этапе проектирования ИТ-продукта[12].
5. Применением механизма доказательств доверия на основе языка событий Event-B и платформы Rodin[13]. Это совместный проект различных команд. Наибольший вклад в его разработку вносят Саутгемптонский университет, компания Systerel и Дюссельдорфский университет.

В настоящее время ни один из них не создает достаточную убедительную систему доказательств доверия к системе ИБ. Последний из рассмотренных средств, методов и технологий (Event-B) уже используется на практике, однако существует ряд проблем его применения[14]:

- Высокий уровень трудозатрат на проведение формальной верификации.
- Ограниченная поддержка командной разработки.
- Отсутствие поддержки выделения часто используемых выражений в отдельные сущности с последующим доступом к ним по ссылке.
- Возможность проявления субъективных оценок и ошибок при написании кода.
- Эта технология не прошла сертификацию ФСТЭК на НДВ и УД.

Но есть и другой подход к созданию системы доверия. С этой точки зрения более интересной является концепция Zero Trust (ZT) – нулевого доверия. Это парадигма кибербезопасности, в которой ни один источник информации и процесс в информационной системе не считаются доверенным без подтверждения [22–24]. Архитектура такой системы информационной безопасности построена на принципе постоянного и полного контроля достоверности источников информации, всех субъектов доступа (пользователи, приложения, устройства) и объектов доступа (корпоративная сеть, интернет, приложения, объекты ввода-вывода информации и другие компоненты информационных систем). Она не исключает использование существующей концепции транзитивного доверия третьей стороны (сертификаты на технические средства защиты информации, SSL, аттестованные объекты информатизации, удостоверяющие центры). Сложность подобно организованных информационных систем в несколько раз превышает сложность обычных систем. Основываясь на этой концепции, можно гарантировать безопасность, в основном, за счёт четырёх аспектов: динамической аутентификации, контроля доступа, непрерывного мониторинга и оценки состояния системы. Эти компоненты тесно сочетаются для реализации системы безопасности.

В настоящее время концепция ZT широко обсуждается в научном сообществе. Практическая реализация этой концепции начата в США в соответствии с указом президента 14028[15] («О повышении кибербезопасности нации»), в котором Федеральному правительству США необходимо начать переход к архитектурам с нулевым доверием в своих инфраструктурах SaaS, PaaS и IaaS. К сожалению, нормативных документов РФ по архитектурам информационных систем с нулевым доверием пока нет, но у нас, как и в мире, эта модель безопасности является активно развивающейся концепцией. В настоящее время широко используется несколько концепций, в том числе NIST [23] и Forrester [24].

11 Приказ ФСТЭК России от 02.06.2020 № 76 «О требованиях по безопасности информации».

12 ГОСТ Р 56939-2024 «Разработка безопасного программного обеспечения».

13 Илья Щепетков, Rodin – платформа для разработки и верификации моделей на Event-B, URL: https://www.ispras.ru/upload/iblock/5e5/5e5ac3663 3ead83d10476199d697be85.pdf (дата обращения: 01.09.2025).

14 Хорошилов А. В., Щепетков И. В. ADV_SPM – Формальные модели политики безопасности на практике. Труды Института системного программирования РАН. 2017;29(3):43–56.

15 US executive order 14028, Improving the Nation's Cyber Security, URL https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity (дата обращения: 01.09.2025).

Они практически отличаются только терминологией и включают следующие основные принципы[16] построения архитектуры ZT [22]:

1. *Безопасность источника данных*. Этот принцип предполагает оценку доверия к источнику информации и его контроль.
2. *Безопасность связи* – связь (канал) должна быть защищена.
3. *Безопасность сеанса* — доступ к ресурсам предоставляется на основе сеанса, а аутентификация и авторизация для одного ресурса не могут предоставлять привилегии другим.
4. *Контроль доступа* — доступ к ресурсам определяется динамической политикой, включая наблюдаемое состояние идентификационных данных клиента, приложения и запрашивающего актива.
5. *Максимальный уровень безопасности* — организация обеспечивает, чтобы все собственные и связанные с ним устройства находились в максимально безопасном состоянии, и отслеживает активы для обеспечения этого.
6. *Непрерывная аутентификация* — все процессы авторизации и аутентификации ресурсов динамические и строго соблюдаются. Организация, планирующая внедрение ZT, может использовать систему управления идентификацией, учётными данными и доступом, а также применять многофакторную аутентификацию для повышения безопасности.
7. *Регистрация информации* — организация собирает как можно больше информации о текущем состоянии сетевой инфраструктуры и коммуникаций и использует эту информацию для повышения уровня своей безопасности.

Анализ возможности применения этих принципов для создания архитектуры ZT коммерческой тайны с учётом требований к её определению и защите, которые были рассмотрены нами ранее в законодательстве США, а также разнообразие форм представления КТ показал, что этих принципов недостаточно и необходимо ввести дополнительно следующие:

1. *Периодическая оценка ценности КТ* на всех этапах её создания, внедрения и применения. Это обеспечивает контроль статуса информации как КТ.
2. *Выделение процессов, в которых используется КТ и персонал*, принимающий в этом участие. Этот принцип позволяет разделить технологические процессы на отдельные выделенные зоны и, тем самым, обеспечить их изолированность и снижение количества сотрудников, включённых в режим КТ.
3. *Обеспечение доказательства утечки КТ*. Реализация только принципа №7 не позволяет полностью реализовать этот принцип и потребует принятия дополнительных технических решений для сбора доказательной базы утечки КТ.
4. *Транзитивность доверия в отношении применяемых сертифицированных средств и технологий*.

16 Знание некоторых принципов освобождает от необходимости знания многих фактов. Клод Адриан Гельвеций.

Классификация форм представления коммерческой тайны и методы их защиты

В настоящее время не существует чёткой классификации форм представления коммерческой тайны. Это является одной из причин отсутствия чётких методических рекомендаций по созданию системы защиты КТ и объясняет появление в законодательстве отдельных стран требований по обеспечению правового режима КТ. Все остальные меры рекомендуется принимать на основе понятий разумности и достаточности. Однако без чёткой классификации построить систему защиты КТ практически невозможно, так как разная форма представления КТ определяет разные механизмы её защиты. Однако выход из этого положения существует, если применить другую парадигму классификации КТ, в которой положена общность механизмов её защиты. Основанная на таком принципе классификация представлена на рис. 1.

В основе любой КТ лежит инновационная идея и это является главным элементом её защиты. Отсюда возникает необходимость защиты инновационных идей на этапе их разработки иначе это может привести к параллельному проектированию КТ, что и происходит во многих случаях. По этой классификации инновационные идеи могут существовать в двух формах: информации и технологий. Носители информации также классифицируются исходя из общих подходов к их защите.

Прежде всего это персонал, обладающий доступом к КТ. Персонал является основным источником утечки информации и разглашения КТ. Технологии организации работы с персоналом по защите секретов в настоящее время достаточно хорошо развиты в отечественных и зарубежных нормативных документах по информационной безопасности [24–25]. Эти технологии основаны на создании: режима конфиденциальности КТ, профессиональной подготовки и обучении, осведомлении, управлении развитием профессиональной этики и поведения персонала при работе с КТ, созданием системы контроля и ответственности за её разглашение.

Класс «информация» разделяется ещё на три класса: материальные носители информации (документы и изделия, содержащие КТ) и электронные носители информации съемные и несъемные. Если материальные носители информации потребуют

Рис. 1. Классификация форм представления коммерческой тайны с позиций общих механизмов её защиты

обычных методов защиты связанные с организацией хранения секретных документов, их учётом и контролем, то электронные носители могут иметь дополнительные технические устройства, обеспечивающие доступ к информации и использование криптографических методов защиты КТ.

Вторая группа классификации «технологии» наиболее сложная и представляет собой несколько классов. Среди них по критерию общих механизмов защиты можно выделить следующие:

1. Информационные технологии, модели и алгоритмы, содержащие КТ. Они должны быть защищены как в процессах разработки, так и в процессах эксплуатации, а также при выводе их из условий эксплуатации. Это обеспечивается применением принципов и механизмов защиты в концепции ZT. В том случае, если эта технология передается по соглашению о нераспространении в другую организацию, необходимо предусмотреть разработку механизмов контроля за её распространением и определения источника несанкционированного распространения КТ. Это может достигаться использованием водяных знаков и скрытой маркировки технологии с использованием стеганографии.
2. Производственные технологии, содержащие КТ. Технологическая линия, в которой используется КТ разделяется на зоны, в которых используется КТ с разной степенью возможного её раскрытия. Проводится анализ каналов утечки информации и проектируются защитные мероприятия по предотвращению утечки производственной информации, составляющей КТ. Одновременно решаются вопросы по созданию режима КТ в отношении персонала, допущенного к КТ. В том случае, если используются информационные технологии, то выполняются меры по защите КТ, рассмотренные в п. 1 этой классификации.
3. При работе с рецептурами и штаммами, отнесенными к КТ необходимо разделить технологию производства на зоны их приготовления и использования. В зонах приготовления рецептур необходимо обеспечить защиту КТ после анализа каналов утечки информации. Кроме того, необходимо обеспечить контроль за распространением и учетом рецептур и штаммов. Принять меры защиты по отношению к персоналу (см. п. 1).

4. Отдельная категория КТ – это совокупность методов и способов обработки данных и специализированных технологий для принятия решений, оптимизации процессов и создания новых продуктов и услуг (BigData). Защита этой категории КТ обеспечивается применением принципов и методов защиты информации в концепции ZT.
5. Категория «искусственный интеллект», как коммерческая тайна, представляет собой технологию виде платформ, обычно на основе нейронных сетей и интерфейсов взаимодействия с ними в форме больших лингвистических моделей. Эти платформы используют для решения задач специальным образом организованные базы данных (DataSet) и Интернет. Вопросы обеспечения безопасности по критериям конфиденциальности, целостности и доступности представляют собой для них серьезную проблему. Если конфиденциальность и доступность этих технологий можно обеспечить, то вопросы их целостности остаются открытыми из-за динамичности изменения состояния баз данных. Это связано и с достоверностью результатов, генерируемых системами ИИ.
6. Организационные технологии также могут быть отнесены к коммерческой тайне. Они представляются обычно в форме концепций, положений, политик, процедур, инструкций, планов, и других документов, применение которых может привести к значительным экономическим эффектам. Электронные формы этих документов защищаются обычными методами с применением криптографических средств и разделением доступа персонала к ним. В качестве примера эффективного применения организационных мер можно привести решение Г. Форда по применению заводского конвейера для сборки автомобилей, что позволило сократить время на производство одного автомобиля с 12 до 1,5 часов[17].

Этапы создания, внедрения и применения коммерческой тайны в организации

Анализ зарубежных и отечественных концепций защиты коммерческой тайны привёл нас к интересному выводу: практически во всех правовых и методических документах КТ рассматривается как некоторое уже готовое решение. Но реально КТ создается не мгновенно, а путем определенной интеллектуальной деятельности, где в основе её всегда лежит некоторая инновационная идея, которая на последующих этапах разработки КТ и её внедрения преобразуются уже в готовое решение. Если эта идея становится общеизвестной, то в этом случае разработка КТ может проходить параллельно в других организациях, что может снизить ожидаемый экономический эффект, а ее правовой статус «коммерческая тайна» будет утерян. Следовательно, защиту КТ необходимо создавать на всех этапах разработки, внедрения и её

17 Форд Г. Генри Форд. Моя жизнь. Мои достижения. – Litres, 2017.

Рис. 2. Полный цикл управления системой защиты коммерческой тайны от её создания до вывода из эксплуатации в концепции ZT

применения. В отдельных случаях необходимо создавать систему защиты информации и при выводе её из эксплуатации. Полный цикл всех этапов разработки КТ от создания инновационных идей до вывода КТ из эксплуатации представлен на рис. 2. Практически не все этапы могут быть пройдены. Это определяется сложностью КТ, научным уровнем ее разработки, трудоемкостью решений и масштабами распространения. В любом случае два этапа «Внедрение КТ» и «Эксплуатация КТ» будут обязательны.

В каждый этап включено моделирование сценариев угроз разглашения (утечки) КТ. Сформулируем условия, при которых выполняются требования концепции ZT.

Пусть p –это процесс связанный с КТ и $p \in P$, t – угроза разглашения КТ и $t \in T$, $d(t)$ – функция доверия к созданию системы защиты от этой угрозы путем принятия мер $m(t)$, которая изменяется в пределах от «0» (отсутствие мер безопасности и полное недоверие) к «1» (полное доверие за счет принятия мер безопасности). Тогда условие реализации ZT для архитектуры ZT будет в следующем виде:

$$\forall p \in P(\neg\exists T(T \in ProcessSets(p) \wedge \\ \wedge (\forall t \in T,\ d(t) = 0),\ m(t) \notin \varnothing))). \quad (1)$$

Если $z(kt)$ – коммерческая ценность продукции, полученной с использованием КТ, а z – коммерческая ценность продукции без применения КТ, тогда условие отнесения ее к коммерческой тайне будет

$$z(kt) >> z\,. \quad (2)$$

При этом должны быть выполнены 11 рассмотренных нами ранее принципов разработки архитектуры безопасности в концепции ZT. На каждом этапе управления КТ моделируются сценарии разглашения (утечки) КТ. В основе моделирования положен анализ процессов работы с КТ и условий их реализации, при которых возможно её разглашение или утечка. Например, при разработке инновационной идеи необходимо определить возможность и необходимость ее обсуждения, формы и технологии её документирования, хранения и распространения. Это позволяет определить каналы возможного распространения КТ и принять необходимые организационные и технические решения, рекомендованные ФСТЭК. Аналогичные подходы к моделированию сценариев разглашения (утечки) КТ применяются и на других этапах управления системой защиты КТ, вплоть до вывода КТ из эксплуатации. Это необходимо в том случае, когда инновационные идеи КТ могут найти новые приложения для практического применения, либо информация является актуальной для дальнейшего использования.

Заключение

Рассмотренные результаты анализа систем защиты информации о коммерческой тайне за рубежом и в России позволяют сделать следующие выводы:

1. Совершенствование защиты коммерческой тайны в России является сегодня одним из важнейших направлений развития научно-технического, технологического, производственного, экономического потенциала страны и укрепление её суверенитета. Эта роль коммерческой тайны в нашей научной среде практически сегодня не обсуждается, хотя такая потребность есть.
2. В настоящее время в мире не существует совершенного законодательства по защите КТ и это связано с разнообразными формами её представления и классификациями, неопределёнными критериями «разумности и достаточности» к её защите. Это является одной из основных проблем в системе управления коммерческой тайной.
3. Современное понятие «коммерческая тайна» распространяется на широкий круг субъектов международных торговых отношений, где в поставляемых нашей страной товарах и изделиях также могут быть тайны, требующие защиты. В нашей научной среде этот вопрос практически не обсуждается, хотя такая потребность также существует.
4. Весьма поверхностно проработаны вопросы применения систем искусственного интеллекта при проектировании КТ [24]. Также требуется совершенствование модели ответственности за разглашение (утечку) КТ. В основу этой модели должен быть положен ущерб, который может понести владелец КТ за её разглашение или утечку.
5. Авторами предложены новые подходы, часть из которых (5a,5b) используется в зарубежных правовых актах, включающие:
   a. Обоснование коммерческой ценности КТ её владельцем, как необходимое условие для защиты КТ государством.
   b. Обязанность владельца КТ по обоснованию разумных и достаточных мер по её технической и организационной защите и доказательства разглашения или утечки КТ.
   c. Классификация КТ с точки зрения общих подходов к её защите.
   d. Обоснование и принципы защиты КТ на основе концепции «нулевого доверия».
   e. Представление КТ в форме циклического управляемого защищаемого процесса от создания инновационной идеи до проектирования, внедрения и эксплуатации КТ. В отдельных случаях обеспечивается защита КТ при выводе её из эксплуатации.

Литература

1. Nashkova S. Defining Trade Secrets in the United States: Past and Present Challenges–A Way Forward? // IIC-International Review of Intellectual Property and Competition Law. – 2023. – Т. 54. – №. 5. – С. 634–672.
2. Desaunettes-Barbero L. Trade Secrets Legal Protection // Munich Studies on. – 2023.
3. Kapczynski A. The public history of trade secrets //UC Davis L. Rev. – 2021. – Т. 55. – С. 1367.
4. O. Ozcan, D. Pickernell and P. Trott, A Trade Secrets Framework and Strategic Approaches, in IEEE Transactions on Engineering Management, vol. 71, pp. 10200–10216, 2024. DOI: 10.1109/TEM.2023.3285292.
5. Kim Y. et al. The effect of trade secrets law on stock price synchronicity: Evidence from the inevitable disclosure doctrine // The Accounting Review. – 2021. – Т. 96. – №. 1. – С. 325–348.
6. Anti-Unfair Competition Law. URL: http://en.npc.gov.cn.cdurl.cn/laws.html (дата обращения: 01.09.2025).
7. Act on Investment Trusts and Investment Corporations https://www.japaneselawtranslation.go.jp/en/laws/view/3605 (дата обращения: 01.09.2025).
8. Федорова Д. А., Котельникова М. А., Старченко А. С. Развитие законодательства Российской Федерации о коммерческой тайне. Порядок возникновения и прекращения права на коммерческую тайну // Международный журнал гуманитарных и естественных наук. – 2023. – № 5 3 (80). – С. 127–131.
9. Балычев А. П. Коммерческая тайна как вид конфиденциальной информации: правовое регулирование в Российской Федерации // Вестник науки. – 2024. – Т. 2. – №. 4(73). – С. 208–218.
10. Федоров П. Г. Формы проявления коммерческой тайны в цифровой экономике // Актуальные проблемы российского права. – 2025. – №. 1(170). – С. 86–97.
11. D. S. Generative artificial intelligence and trade secrecy // J. Free Speech L. – 2023. – Т. 3. – С. 559.
12. Слицкая А. Е. Использование генеративного искусственного интеллекта в SEO для электронной коммерции // Инновации и инвестиции. – 2023. – №. 11. – С. 326–329.
13. Столяров А. Д., Абрамов В. И., Абрамов А. В. Генеративный искусственный интеллект для инноваций бизнес-моделей: возможности и ограничения // Beneficium. – 2024. – № 3 (52). – С. 43–51.
14. Половинкин А. И. Основы инженерного творчества / А. И. Половинкин; Издательство: Лань. Серия. Техника. ТехниЛань; науки в целом. 2022. – 360 с.
15. Рубин М. С. Основы ТРИЗ для предприятий. М.: КТК «Галактика». 2022. – 354 с.
16. Rajendran, S., & Shankar, K. Artificial Intelligence Techniques for Cybersecurity. Security and Privacy, 2021. 4(1), e122.
17. Брабанд Й., Шебе Х. Оценка безопасности искусственного интеллекта // Надежность. – 2020. – Т. 20. – №. 4. – С. 25–34.
18. Артамонов В. А., Артамонова Е. В., Сафонов А. Е. Безопасность искусственного интеллекта // Защита информации. Инсайд. – 2022. – №. 6(108). – С. 8.
19. Hrdy, Camilla Alexandra, Trade Secrets and Artificial Intelligence (July 14, 2025). Rutgers Law School Research Paper, Trade Secrets and Artificial Intelligence Forthcoming in Elgar Concise Encyclopedia of Artificial Intelligence and the Law (Edward Elgar, eds. Ryan Abbott, Elizabeth Rothman, forthcoming, 2026), Available at SSRN: https://ssrn.com/abstract=5350892 or http://dx.doi.org/10.2139/ssrn.5350892 (дата обращения: 01.09.2025).
20. Ротман Дэнис. RAG и генеративный ИИ. Создаем собственные RAG-пайплайны с помощью LlamaIndex, Deep Lake и Pinecon. – Астана: «Спринт Бук», 2025. – 320 с.: ил. ISBN 978-601-12-3149-7.
21. Theory and Application of Zero Trust Security: A Brief Survey by Hongzhaoning Kang 1ORCID, Gang Liu 1, Quan Wang, Lei Meng and Jing Liu – November 2023 https://www.mdpi.com/1099-4300/25/12/1595 (дата обращения: 01.09.2025).
22. Seefeldt J. what's new in nist zero trust architecture // NIST Special Publication. – 2021. – Т. 800. – С. 207.
23. Gangina P. Demystifying Zero-Trust Architecture for Cloud Applications // Journal of Computer Science and Technology Studies. – 2025. – Т. 7. – №. 9. – С. 542–548.
24. Oforleta, Chibuzor, Reassessing Trade Secret Protections in the Era of AI: A Comparative Perspective on Legal and Ethical Challenges (February 18, 2025). Available at SSRN: https://ssrn.com/abstract=5143701 or http://dx.doi.org/10.2139/ssrn.5143701 (дата обращения: 01.09.2025).

IMPROVING THE TRADE SECRET PROTECTION SYSTEM: PRINCIPLES, CLASSIFICATION, METHODS, AND TECHNOLOGIES

Minzov A. S.[18], Nevsky A. Yu.[19], Minzov S. A.[20]

Keywords: *trade secret, information security system, trade secret regime, zero trust.*

Study objective: *to substantiate a system for protecting trade secrets in various forms based on classification, principles, methods, and technologies.*

Research methods: *a retrospective analysis of trade secret protection requirements in Russia and abroad; a systems analysis to substantiate trade secret classification; conceptual modeling of a trade secret protection system based on the Zero Trust concept; and a synthesis of a trade secret protection system at all stages of its life cycle.*

Study results: *the obtained results do not contradict existing regulatory documents on trade secret protection and can be used to enhance the protective properties of various objects where the need to protect trade secrets arises in Russia and abroad.*

18 Anatoly S. Minzov, Dr.Sc. of Technical Sciences, Professor, National Research University MPEI, Moscow, Russia. E-mail: MinzovAS@mpei.ru
19 Alexander Yu. Nevsky, Ph.D. of Technical Sciences, Associate Professor, National Research University MPEI, Moscow, Russia. E-mail: NevskiyAY@mpei.ru
20 Stepan A. Minzov, Deputy Head of the ACS (DB) Department, JSCB «ForaBank», Moscow, Russia. E-mail: minzov@forabank.ru

Scientific novelty: *the article proposes new approaches to classifying trade secrets from the perspective of protecting them from disclosure (leakage), principles for protecting trade secrets based on the "zero trust" concept, and a trade secret protection management system as a cyclical, controlled, and protected process from the creation of an innovative idea, through design, implementation, and operation.*

Practical relevance: *the authors' proposed solutions and approaches to protecting trade secrets will improve the level of security for economic entities where protection is necessary, increase innovative activity in market relations, and counter industrial and economic espiona.*

References

1. Nashkova S. Defining Trade Secrets in the United States: Past and Present Challenges–A Way Forward? // IIC-International Review of Intellectual Property and Competition Law. – 2023. – T. 54. – №. 5. – S. 634–672.
2. Desaunettes-Barbero L. Trade Secrets Legal Protection // Munich Studies on. – 2023.
3. Kapczynski A. The public history of trade secrets // UC Davis L. Rev. – 2021. – T. 55. – S. 1367.
4. O. Ozcan, D. Pickernell and P. Trott, A Trade Secrets Framework and Strategic Approaches, in IEEE Transactions on Engineering Management, vol. 71, pp. 10200–10216, 2024. DOI: 10.1109/TEM.2023.3285292.
5. Kim Y. et al. The effect of trade secrets law on stock price synchronicity: Evidence from the inevitable disclosure doctrine // The Accounting Review. – 2021. – T. 96. – №. 1. – S. 325–348.
6. Anti-Unfair Competition Law. URL: http://en.npc.gov.cn.cdurl.cn/laws.html (data obrashhenija: 01.09.2025).
7. Act on Investment Trusts and Investment Corporations https://www.japaneselawtranslation.go.jp/en/laws/view/3605 (data obrashhenija: 01.09.2025).
8. Fedorova D. A., Kotel'nikova M. A., Starchenko A. S. Razvitie zakonodatel'stva Rossijskoj Federacii o kommercheskoj tajne. Porjadok vozniknovenija i prekrashhenija prava na kommercheskuju tajnu // Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk. – 2023. – № 53(80). – S. 127–131.
9. Balychev A. P. Kommercheskaja tajna kak vid konfidencial'noj informacii: pravovoe regulirovanie v Rossijskoj Federacii // Vestnik nauki. – 2024. – T. 2. – №. 4(73). – S. 208–218.
10. Fedorov P. G. Formy projavlenija kommercheskoj tajny v cifrovoj jekonomike // Aktual'nye problemy rossijskogo prava. – 2025. – №. 1 (170). – S. 86–97.
11. D. S. Generative artificial intelligence and trade secrecy // J. Free Speech L. – 2023. – T. 3. – S. 559.
12. Slickaja A. E. Ispol'zovanie generativnogo iskusstvennogo intellekta v SEO dlja jelektronnoj kommercii // Innovacii i investicii. – 2023. – №. 11. – S. 326–329.
13. Stoljarov A. D., Abramov V. I., Abramov A. V. Generativnyj iskusstvennyj intellekt dlja innovacij biznes-modelej: vozmozhnosti i ogranichenija // Beneficium. – 2024. – № 3 (52). – S. 43–51.
14. Polovinkin A. I. Osnovy inzhenernogo tvorchestva / A. I. Polovinkin; Izdatel'stvo: Lan'. Serija. Tehnika. TehniLan'; nauki v celom. 2022. – 360 s.
15. Rubin M. S. Osnovy TRIZ dlja predprijatij. M.: KTK «Galaktika». 2022. – 354 s.
16. Rajendran, S., & Shankar, K. Artificial Intelligence Techniques for Cybersecurity. Security and Privacy, 2021. 4(1), e122.
17. Braband J., Shebe H. Ocenka bezopasnosti iskusstvennogo intellekta // Nadezhnost'. – 2020. – T. 20. – №. 4. – S. 25–34.
18. Artamonov V. A., Artamonova E. V., Safonov A. E. Bezopasnost' iskusstvennogo intellekta // Zashhita informacii. Insajd. – 2022. – №. 6(108). – S. 8.
19. Hrdy, Camilla Alexandra, Trade Secrets and Artificial Intelligence (July 14, 2025). Rutgers Law School Research Paper, Trade Secrets and Artificial Intelligence Forthcoming in Elgar Concise Encyclopedia of Artificial Intelligence and the Law (Edward Elgar, eds. Ryan Abbott, Elizabeth Rothman, forthcoming, 2026), Available at SSRN: https://ssrn.com/abstract=5350892 or http://dx.doi.org/10.2139/ssrn.5350892 (data obrashhenija: 01.09.2025).
20. Rotman Djenis. RAG i generativnyĭ II. Sozdaem sobstvennye RAG-paĭplaĭny s pomoshh'ju LlamaIndex, Deep Lake i Pinecon. Astana: Sprint Buk. 2025. 320 s.: il. ISBN 978-601-12-3149 7.
21. Theory and Application of Zero Trust Security: A Brief Survey by Hongzhaoning Kang 1ORCID, Gang Liu 1, Quan Wang, Lei Meng and Jing Liu – November 2023 https://www.mdpi.com/1099-4300/25/12/1595 (data obrashhenija: 01.09.2025).
22. Seefeldt J. what's new in nist zero trust architecture // NIST Special Publication. – 2021. – T. 800. – S. 207.
23. Gangina P. Demystifying Zero-Trust Architecture for Cloud Applications // Journal of Computer Science and Technology Studies. – 2025. – T. 7. – №. 9. – S. 542–548.
24. Oforleta, Chibuzor, Reassessing Trade Secret Protections in the Era of AI: A Comparative Perspective on Legal and Ethical Challenges (February 18, 2025). Available at SSRN: https://ssrn.com/abstract=5143701 or http://dx.doi.org/10.2139/ssrn.5143701 (data obrashhenija: 01.09.2025).