Владислав Владимирович Просяник

кандидат политических наук, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, v.v.prosyanik@utmn.ru

Виктория Сергеевна Табурчак

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, taburchakvictoria@mail.ru

Сания Еркешевна Купбаева

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, saniiusha9@gmail.com

СОВРЕМЕННЫЕ ПОДХОДЫ К СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Аннотация. Статья посвящена исследованию современных подходов к обеспечению сохранности коммерческой тайны в условиях цифрового общества, с акцентом на IT-компании как ключевые хозяйствующие субъекты. На основе сравнительного анализа выявляются правовые, организационные и технические аспекты защиты конфиденциальной информации, включая внутренние (злоупотребления персонала) и внешние угрозы (кибератаки, утечки через облачные сервисы). На примере реального кейса компании Samsung продемонстрированы катастрофические последствия нарушения сохранности коммерческой тайны: финансовые потери, репутационные риски, снижение конкурентного преимущества. Автор доказывает необходимость интеграции технологических решений и организационных мер для минимизации рисков. Особое внимание уделяется совершенствованию правового регулирования коммерческой тайны, включая адаптацию законодательства к вызовам цифровизации. Результаты исследования подчеркивают, что устойчивость экономической безопасности IT-компаний напрямую зависит от своевременной модернизации подходов к защите данных.

Ключевые слова: коммерческая тайна, экономическая безопасность, конфиденциальность, IT-компании, киберугрозы, цифровая трансформация.

Vladislav Vladimirovich Prosyanik

Candidate of Sciences (Political), Associate Professor of the Department of Economic Security, System Analysis and Control, University of Tyumen, Tyumen, v.v.prosyanik@utmn.ru

Victoria Sergeevna Taburchak

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, taburchakvictoria@mail.ru

Saniia Erkeshevna Kupbaeva

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, saniiusha9@gmail.com

MODERN APPROACHES TO THE PRESERVATION OF TRADE SECRETS IN ORDER TO ENSURE ECONOMIC SECURITY OF AN ECONOMIC ENTITY

Abstract. The article is devoted to the study of modern approaches to ensuring the safety of trade secrets in a digital society, with an emphasis on IT companies as key business entities. Based on a comparative analysis, legal, organizational, and technical aspects of protecting confidential information are identified, including internal (personnel abuse) and external threats (cyber-attacks, leaks through cloud services). Using the example of a real Samsung case, the catastrophic consequences of violating trade secrets are demonstrated: financial losses, reputational risks, and reduced competitive advantage. The

author proves the need to integrate technological solutions and organizational measures to minimize risks. Special attention is paid to improving the legal regulation of trade secrets, including adapting legislation to the challenges of digitalization. The results of the study emphasize that the sustainability of the economic security of IT companies directly depends on the timely modernization of approaches to data protection.

Keywords: trade secret, economic security, confidentiality, IT companies, cyber threats, digital transformation.

На сегодняшний день даже небольшие предприятия используют IT-инфраструктуру для хранения, обработки и передачи важной информации. Эпоха цифровизации изменила подходы к ведению бизнеса кардинальным образом и бумажные носители ушли на второй план. В связи с этим появились риски хранения информации, в том числе коммерческой тайны предприятия.

С экономической точки зрения, коммерческая тайна — это сведения (производственные, технические, экономические), которые представляют собой коммерческую ценность и предоставляют предпринимателю определенное преимущество в конкурентной борьбе, но только до тех пор, пока они содержатся в секрете и неизвестны третьим лицам [1, с. 50].

С юридической точки зрения, коммерческая тайна — это режим конфиденциальности информации, 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 [2, с. 50].

В РФ отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны регулируются федеральным законом «О коммерческой тайне» от 29.07.2004 № 98-ФЗ. В соответствии с федеральным законом № 98-ФЗ владельцем коммерческой тайны признается лицо, которое на законных основаниях владеет сведениями, составляющими коммерческую тайну, ограничивает доступ к этой информации и устанавливает режим коммерческой тайны в отношении нее.

Владелец информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Информация, которая не подлежит разглашению, то есть является конфиденциальной, определяется руководителем хозяйствующего субъекта. Выделяются следующие виды информации, которые составляют коммерческую тайну (рис. 1):

– научно-техническая информация;
– технологическая информация;
– производственная информация;
– финансово-экономическая информация;
– информация, составляющая секреты производства (ноу-хау);
– иная информация, обладающая потенциальной либо действительной ценностью.

Рис. 1. Виды информации, составляющие коммерческую тайну

Источник: [3, с. 56].

Так, современная коммерческая тайна все чаще включает в себя данные, обеспечивающее конкурентное преимущество: исходный код, алгоритмы машинного обучения, пользовательские метаданные, стратегии разработки, что создает принципиально новые риски:

– возможность моментальной копии и передачи конфиденциальных данных;
– уязвимость к внешним кибератакам;
– риски, связанные с человеческим фактором (например, передача информации через мессенджеры).

Угрозы в экономической безопасности для предприятия представляют собой обстоятельства и факторы, которые препятствуют компаниям достигать целей в экономической сфере. Они создают трудности для реализации ее интересов и могут создавать обстоятельства, при которых хозяйствующий субъект несет убытки в деятельности, ухудшается финансовое состояние и стабильность.

Для более точного понимания угроз при нарушении коммерческой тайны необходимо рассмотреть их виды, типы и источники возникновения (табл. 1). Внутренние угрозы связаны с персоналом компании. Сотрудники, имеющие доступ к корпоративной информации, могут присвоить и распространить данные, составляющие коммерческую тайну. Внешние угрозы имеют несколько групп субъектов, которые могут проявлять интерес к получению коммерческих сведений. К ним относятся конкуренты, действующие на тех же рынках, а также субъекты, которые борются за активы и доли предприятия. Кроме того, существуют смешанные угрозы, которые включают в себя особенности и внутренних, и внешних угроз.

Таблица 1

Виды угроз при нарушении коммерческой тайны и их классификация

Категория угроз	*Тип угрозы*	*Примеры*	*Источники или причины возникновения*
1	*2*	*3*	*4*
Внутренние угрозы	Умышленные действия	– продажа данных конкурентам; – саботаж (утечка из-за конфликтов); – копирование информации перед увольнением	– недовольство сотрудников; – коррупция; – отсутствие контроля за увольняющимися
	Неосторожное обращение	– отправка файлов на личную почту; – использование незащищенных мессенджеров; – потеря устройств	– недостаточное обучение ИБ; – пренебрежение правилами безопасности
	Системные недостатки	– отсутствие разграничения доступа; – устаревшие регламенты; – непроведение аудитов	– неэффективная ИБ-политика; – недофинансирование защиты данных
Внешние угрозы	Кибератаки	– взлом серверов (фишинг, вирусы); – перехват данных (атаки на VPN); – DDoS-атаки	– уязвимости ПО; – слабые пароли; – отсутствие обновлений защиты
	Промышленный шпионаж	– внедрение агентов в штат; – подкуп сотрудников; – техническое наблюдение (жучки)	– деятельность конкурентов; – недостаточная проверка персонала

Окончание табл. 1

1	*2*	*3*	*4*
	Партнерские риски	– утечки через подрядчиков; – нарушение конфиденциальности в совместных проектах	– непроверенные контрагенты; – слабое юридическое сопровождение сделок
Смешанные угрозы	Комбинированные	– уход сотрудников к конкурентам с данными; – утечки через бывших работников	– несвоевременное отключение доступа; – недостатки в системе мониторинга
	Удаленные рабочие места	– компрометация личных устройств; – доступ к данным через незащищенные сети	– отсутствие VPN/шифрования; – несоблюдение политики BYOD (Bring Your Own Device)

Источник: составлено авторами на основе данных [4].

Также стоит выделить проблемы и угрозы, которые возникают в результате нарушения режима коммерческой тайны в IT-компаниях, это:

1) Финансовые потери. Это характеризуется снижением рыночной стоимости компании в связи с утечкой ноу-хау.

2) Репутационные риски. Их возникновение подразумевает под собой потерю доверия клиентов и инвесторов.

3) Юридические последствия. К ним относятся штрафы за несоблюдение GDPR или ФЗ-152.

4) Удаленная работа. Является угрозой, которая может повлечь за собой утечку информации компании. Например, в 2023 году 43% утечек произошли через личные устройства сотрудников.

Угрозы экономической безопасности предприятия могут нанести значительный ущерб его деятельности, финансовой стабильности и репутации. Анализ источников и типов угроз показывает, что их последствия могут включать финансовые потери, репутационные риски, юридические санкции и утечку данных через удаленные рабочие места или открытые платформы. Согласно исследованиям экспертного сообщества, 93% опрошенных респондентов из российского бизнес-сообщества сталкивались с двумя и более видами корпоративного мошенничества, из них: кража/утечки инсайдерской, конфиденциальной информации, персональных данных или интеллектуальной собственности — 29%, киберпреступления (фишинг, DDoS-атаки, хакерские атаки, иные виды кибер-угроз) — 14%.

Для предотвращения негативных последствий важно внедрять комплексные меры защиты, включая разработку политики информационной безопасности, обучение сотрудников, мониторинг потенциальных рисков и использование современных технологий для защиты корпоративной информации. Только системный подход позволит минимизировать угрозы и обеспечить устойчивое развитие предприятия в условиях современного рынка.

В марте 2023 года в компании Samsung произошла масштабная утечка корпоративных данных. Сотрудники компании использовали ChatGPT для оптимизации своей работы: загружали в систему фрагменты исходного кода, патентные описания и протоколы встреч. Вследствие этого конфиденциальные данные утекли в сеть, что сделало их потенциально доступными для третьих лиц [5]. Это привело к угрозе утечки ключевых технологий, включая разработки в области полупроводников и ИИ. Причинами инцидента стали отсутствие четко регламента по использованию публичных ИИ-инструментов для работы с коммерческой тайной и недостаточная осведомленность сотрудников о рисках взаимодействия с искусственным интеллектом. Естественно, был нанесен репутационный ущерб, который выразился в снижении доверия партнеров, клиентов и инвесторов к корпоративной безопасности Samsung. Компания же в свою очередь предупредила сотрудников, что с чат-ботами нельзя делиться конфиденциальной информацией, а также любыми данными, которые могут навредить корпорации, ввела некоторые ограничения на вопросы, задаваемые в ChatGPT, и, даже рассмотрела возможность создания собственного внутреннего чат-бота, чтобы предотвратить утечки.

Второй кейс касается уже внутренних угроз при нарушении коммерческой тайны, о которых упоминалось ранее. «Южнокорейская полиция арестовала двух бывших топ-менеджеров компании, подозреваемых в утечке секретных данных Samsung на сумму $3,2 млрд» [6]. Бывшие топ-менеджеры Samsung, обладая знаниями, полученными в годы работы в компании, создали в Китае предприятие по производству чипов, скопировав технологии 20-нм DRAM. Такая утечка лишила Samsung конкурентного преимущества. Это не первый случай задержания сотрудника южнокорейской технологической компании за кражу коммерческой тайны.

Оба кейса демонстрируют, что даже такие крупные компании как Samsung, десятилетиями ассоциировавшиеся с надежностью и инновациями, сталкиваются с катастрофическими рисками при несоблюдении современных требований к защите коммерческой тайны. Для предотвращения подобных инцидентов требуется интеграция технологических и организационных мер. Стоит понимать, что, когда искусственный интеллект «поглощает» конфиденциальную информацию компании, а бывшие сотрудники воссоздают технологии для конкурентов, компания теряет не просто информацию — она теряет будущее.

Исходя из вышесказанного, современные «вызовы» требуют комплексных решений, которые будут объединять инновационные технологии и обновление внутренних процессов хозяйствующих субъектов. Разберем какие есть современные подходы к сохранению коммерческой тайны, которые позволят не только снизить риск утечки конфиденциальной информации, но и усилят значение компании в цифровой экономике, где данные определяют конкурентное превосходство.

Технологические решения включают внедрение DLP-систем, программно-аппаратного комплекса, предназначенного для обнаружения и предотвращения несанкционированной передачи конфиденциальной информации за пределы корпоративной сети. Проще говоря, это система, контролирующая все информационные потоки компании [7]. Кроме того, компания Zecurion разработала

комплексную систему защиты DLP от утечек корпоративной информации. Ее особенность — фокусирование на психологических аспектах, при котором система помогает выявлять потенциально опасных сотрудников еще до того, как они решат слить информацию.

Существует также Zero Trust-архитектура — подход к кибербезопасности, предполагающий отсутствие заранее предоставленного доверия любому субъекту внутри или снаружи сети. То есть каждый пользователь, устройство или процесс должны пройти проверку и получить разрешение на доступ к определенным ресурсам. Эта концепция предназначена для предотвращения утечек данных от кибератак и обеспечения должного уровня защиты информации [8].

Под организационными мерами предполагается обновление политик коммерческой тайны с запретом на использование ChatGPT и аналогичных инструментов для работы с конфиденциальными данными. Помимо этого, обязательным фактором является и обучение сотрудников. Программа обучения может включать в себя:

– тренинги по кибергигиене — распознавание фишинга, социальной инженерии, правил работы с облачными сервисами;

– симуляции утечек — моделирование атак через поддельные письма или «утечку» тестовых данных для оценки реакции сотрудников;

– обучение работе с DLP-системами — разъяснение принципов блокировки подозрительных действий.

Таким образом, интеграция технологических и организационных мер создает многоуровневую систему защиты коммерческой тайны. DLP-системы и Zero Trust минимизируют технические риски, а обновленные политики и обучение снижают вероятность человеческих ошибок. Только такой комплексный подход позволяет компаниям сохранить экономическую безопасность в условиях цифровизации и глобальной конкуренции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Башаримов, И.С. Коммерческая деятельность: учебное пособие / И.С. Башаримов. — Москва: Велби, 2017. — 336 с.
2. Валюженич, Н. Коммерческая тайна: предпринимательство и лояльность персонала: учебное пособие / Н. Валюженич. — Москва: Инфра-М, 2015. — 445 с.
3. Гапоненко, В.Ф. Экономическая безопасность предприятий. Подходы и принципы / В.Ф. Гапоненко. — Москва: Велби, 2014. — 340 с.
4. Защита информации, составляющей коммерческую тайну // Searchinfo.rm: сайт — URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/zaschita-informatsii-sostavlyayuschej-kommercheskuyu-tajnu/ (дата обращения: 12.04.2025).
5. Вот и поговорили: почему из-за чат-ботов происходят утечки данных // Известия: сайт. — URL: https://iz.ru/1494443/dmitrii-bulgakov/vot-i-pogovorili-pochemu-iz-za-chat-botov-proiskhodiat-utechki-dannykh (дата обращения: 12.04.2025).
6. Экс-руководителей Samsung арестовали за передачу данных Китаю // Хабр: сайт. — URL: https://habr.com/ru/news/842354/ (дата обращения: 12.04.2025).
7. Что такое DLP-система информационной безопасности // Gartel: сайт. — URL: https://www.gartel.ru/articles/dlp-sistema/ (дата обращения: 12.04.2025).
8. Что такое Zero Trust и почему это будущее безопасности сайтов // Интернет хостинг центр: сайт. — URL: https://www.ihc.ru/articles/chto-takoe-zero-trust-i-pochemu-eto-budushhee-bezopasnosti-sajtov.html (дата обращения: 12.04.2025).