УДК 004.8:338:658


## OSINT в оценке рисков для юридических лиц

А.Д. Зайцева
студент 2 курса бакалавриата НИЯУ МИФИ, Москва
Email: zaycevasa.12@mail.ru
М.С. Бугаков
студент 2 курса бакалавриата НИЯУ МИФИ, Москва
Email: mishabugakov689@gmail.ru
В.А. Романовский
ассистент кафедры финансового мониторинга НИЯУ МИФИ, Москва
Email: VARomanovskii@mephi.ru

Аннотация: *В данной работе рассмотрено применение техник разведки по открытым источникам (OSINT) с целью оценки рисков для юридических лиц. Авторами обозначены ключевые категории угроз и методики их выявления посредством проведения разведки по открытым источникам. Особое внимание уделено правовым аспектам и практической интеграции OSINT в систему риск-менеджмента компаний.*

Ключевые слова: *OSINT, оценка рисков, бизнес, конкурентная разведка, разведка по открытым источникам, риск-менеджмент*

## OSINT in risk assessment for legal entities

A.D. Zayceva
2st year student at NRNU MEPhI, Moscow
Email: zaycevasa.12@mail.ru
M.S. Bugakov
2st year student at NRNU MEPhI, Moscow
Email: mishabugakov689@gmail.ru
V.A. Romanovsky
Assistant of the Department of Financial Monitoring
NRNU MEPhI, Moscow
Email: VARomanovskii@mephi.ru

Abstract: *This paper examines the use of open source intelligence (OSINT) techniques to assess risks for legal entities. The authors identify key categories of threats and methods for detecting them through open source intelligence. Special attention is paid to the legal aspects and practical integration of OSINT into the company's risk management system.*

Keywords: *OSINT, risk assessment, business, competitive intelligence, open source intelligence, risk management*

Введение

В условиях цифровой трансформации и глобализации бизнес-среды юридические лица всё чаще сталкиваются с ростом различного рода угроз, начиная от репутационных кризисов и заканчивая кибератаками. Традиционные методы оценки рисков зачастую оказываются недостаточно оперативными и всеобъемлющими, особенно когда речь идет о скрытых или слабоструктурированных данных. В этой связи разведка по открытым источникам (OSINT – open source intelligence) становится критически важным инструментом для превентивного анализа и управления рисками.

Ключевым достоинством данного подхода выступает возможность выявления угроз на ранних стадиях, используя доступные всем данные из публичных источников информации: от государственных реестров до социальных сетей. Однако, несмотря на широкие возможности, многие компании при работе с данным инструментом сталкиваются с проблемами хранения и анализа данных, их верификации и соблюдения правовых норм.

Цель исследования — определить такие техники OSINT-разведки, которые эффективны для оценки рисков юридических лиц, предложить пошаговую методику анализа и дать рекомендации по их внедрению и реализации.

Задачи исследования:

- Определить категории рисков, выявляемых с помощью OSINT-техник.
- Проанализировать основные источники открытых данных и инструменты для их обработки.
- Разработать алгоритм оценки угроз на основе OSINT.
- Рассмотреть правовые и этические аспекты работы с открытыми источниками.

Методология исследования включает анализ научных публикаций, обзор современных OSINT-инструментов, а также изучение реальных кейсов из корпоративной практики.

Теоретические основы OSINT в оценке рисков. В наше время значительный объем данных, доступных из онлайн-источников, изменил способы сбора и анализа информации. Появление Интернета и стремительный рост онлайн-платформ привели к значительному увеличению объема доступных данных. Сегодня OSINT играет важную роль в оценке рисков, обеспечивая всестороннее понимание внешних факторов, которые могут повлиять на функционирование современного бизнеса. Используя OSINT, управляющие лица могут принимать обоснованные решения на основе всесторонней и актуальной информации, что в конечном

итоге повышает их способность защищать активы, репутацию и позволяет обеспечить должный уровень финансовой и экономической безопасности.
Ключевые преимущества использования OSINT в управлении рисками:

- Во-первых, OSINT представляет собой экономичную альтернативу традиционной аналитике, в том числе методам сбора данных, которые могут отнимать много времени и ресурсов. Используя общедоступную информацию, организации могут получать доступ к ценным сведениям без необходимости значительных финансовых вложений.
- Во-вторых, OSINT позволяет осуществлять более широкий и всесторонний сбор информации, что позволяет аналитикам получить целостное представление о рисках, что повышает точность и полноту оценки рисков, сокращая количество "белых пятен" и способствуя активному управлению рисками.
- Кроме того, OSINT способствует гибкости и адаптивности в оценке рисков. Он дает возможность собирать и анализировать данные в режиме реального времени и своевременно обнаруживать потенциальные угрозы и уязвимости, что позволяет принимать предупреждающие меры и минимизировать потенциальный ущерб. [4]

Основные риски юридических лиц и роль OSINT. В современной конкурентной среде юридические лица сталкиваются с большим рядом угроз, способных нанести весомый ущерб их репутации, финансовому состоянию и операционной деятельности. OSINT становится мощным инструментом для выявления, анализа и минимизации этих рисков. Рассмотрим ключевые категории угроз, с которыми сталкиваются компании, и способы их обнаружения с помощью открытых данных.

Основные группы рисков, которые выделяет бизнес [1]:

1. Репутационные риски.

Репутация компании — ее потеря может привести к оттоку клиентов, партнеров и инвесторов. OSINT в данном случае позволяет компании:

- Осуществлять мониторинг упоминаний в СМИ, соцсетях и на форумах.
- Выявлять фейковые аккаунты и мошеннические схемы, использующие бренд компании.
- Анализировать настроения аудитории для прогнозирования кризисных ситуаций.
- Наблюдать за скандалами компаний-конкурентов и на их опыте идентифицировать и корректировать собственные слабые места, чтобы предотвратить наступление схожих обстоятельств.

2. Финансовые и экономические риски.

К серьезным убыткам также может привести работа с неблагонадёжными партнерами. С помощью OSINT можно:

- Проверять благонадежность партнеров через открытые реестры (ЕГРЮЛ, Федресурс, ГИРБО). [2]

- Анализировать судебные базы данных (Кадарбитр, Судебные решения РФ) на наличие исков и банкротств партнеров. [2]
- Отслеживать изменения в структуре собственности компаний, выявляя подставные фирмы и схемы незаконной оптимизации налогов и сборов.

3. Операционные риски и киберугрозы.

Усложнить процессы компании могут также уязвимости в IT-инфраструктуре. OSINT помогает:

- Отслеживать отсутствие утечки данных во всемирной паутине.
- Анализировать открытые технические данные для выявления уязвимых серверов и доменов.
- Осуществлять мониторинг активности хакерских группировок, открыто обсуждающих целевую атаку на компанию.
- Изучать подробности атак на другие компании и на основе этого выявлять свои слабые места и работать над нами.

4. Правовые и регуляторные риски.

Нарушения законодательства могут привести к штрафам и судебным искам, то есть повышению издержек, торможению процессов и ухудшению репутации компании. OSINT позволяет:

- Контролировать соблюдение compliance-требований.
- Отслеживать изменения в законодательстве.
- Следить за случаями нарушениями законодательства другими компаниями, чтобы исключить подобные обстоятельства в собственной финансово-хозяйственной деятельности. [4]

5. Конкурентные риски и промышленный шпионаж.

Также компании необходимо отслеживать нововведения на рынке и не отставать от конкурентов. С помощью OSINT можно:

- Анализировать вакансии конкурентов для прогнозирования их стратегий.
- Осуществлять мониторинг патентных баз и научно-публикационной активности на предмет новых, востребованных технологий.
- Отслеживать упоминание новых проектов конкурентов в СМИ.

6. Физические риски.

Для компаний с глобальным присутствием или работающих в нестабильных регионах мониторинг физической безопасности становится критически важным элементом риск-менеджмента. OSINT предоставляет такие возможности:

- Мониторинг криминальной обстановки через местные и региональные СМИ, полицейских сводок и криминальных форумов.
- Прогнозирование протестной активности путем отслеживания социальных сетей и мессенджеров.

- Оценка природных рисков с использованием данных метеослужб и отчетов МЧС.
- Контроль транспортных маршрутов посредством мониторинга дорожной ситуации и сообщений перевозчиков.

Таким образом, OSINT становится неотъемлемой частью системы риск-менеджмента, обеспечивая комплексную защиту бизнеса от различного рода рисков. Внедрение OSINT-техник позволит повысить эффективность применения риск-ориентированного подхода.

Ситуационный анализ (СА) позволяет организовывать и направлять процесс активного сбора, оценки и переработки имеющейся первичной информации и воспроизводства новой, вторичной информации как аналитического, так и прогнозного характера.

Ситуационный подход можно представить состоящим из следующих основных составляющих:

1. Изучение современных технологий ситуационного анализа.
2. Предвидение последствий принимаемых решений.
3. Интерпретация ситуации с выделением наиболее важных факторов (переменных) и оценкой возможных последствий их изменения.
4. Принятие эффективного решения.

Методы ситуационного анализа в сочетании с OSINT-техниками позволяет проводить полномасштабную конкурентную разведку.

Основные источники OSINT для бизнеса и оценки рисков.

Современные компании могут использовать открытые источники информации для комплексного анализа ситуации и возможных рисков, конкурентной разведки и стратегического планирования. Ключевые категории источников, которые помогают бизнесу получать данные для принятия решений [3]:

1. Открытая отчетность компаний (Государственные реестры (ЕГРЮЛ, Федресурс), корпоративные сайты и базы данных (СПАРК))

Они содержат информацию о собственниках, финансовых показателях, судебных исках и истории изменений в структуре бизнеса. Анализ этих данных помогает:

- выявлять ненадежных контрагентов
- оценивать устойчивость партнеров. [2]

2. Поисковые системы (Google, Yandex, Bing)

Позволяют:

- Отслеживать репутацию по публикациям в СМИ и на форумах
- Анализировать конкурентные предложения в выдаче поиска
- Находить скрытые страницы и документы (операторами поиска)

3. Социальные сети (Telegram, VK и другие)

Используются для:

- Анализа активности конкурентов (акции, реклама, PR-стратегии)
- Изучения отзывов клиентов и выявления репутационных рисков

- Поиска утечек внутренней информации через сотрудников

4. Сайты-отзовики (Flamp, Otzovik, Trustpilot, PissedConsumer)

Позволяют оценить:

- Уровень удовлетворенности клиентов и репутацию компании
- Типичные жалобы на продукт или сервис
- Возможные фейковые отзывы (заказные, конкурентные)

5. Онлайн-карты (Google Maps, Yandex.Карты, 2GIS)

Дают возможность:

- Сравнить локации конкурентов и их инфраструктуру
- Проанализировать отзывы о точках продаж (своих и конкурентов)
- Выявить динамику развития сети (новые открытия/закрытия)

6. СМИ и новостные агрегаторы (Коммерсантъ, региональные издания)

Полезны для:

- Отслеживания публикаций о конкурентах (интервью, скандалы, судебные иски) и о себе
- Мониторинга изменений в законодательстве, влияющих на бизнес
- Выявления негативных новостей до их масштабного распространения

7. Форумы, отраслевые выставки и конференции

Позволяют:

- Находить экспертные обсуждения технологий и рыночных трендов
- Выявлять слабые места конкурентов и своей компании через мнения профессионалов
- Узнавать о новых продуктах до их официального анонса

8. Тайные покупатели (Mystery Shopping, собственные проверки)

Метод помогает:

- Оценить качество сервиса конкурентов
- Протестировать реальные условия продаж и выполнения заказов
- Выявить скрытые маркетинговые уловки

9. Анализ вакансий (HH.ru, LinkedIn, Rabota.ru)

Позволяет определить:

- Планы компании по расширению (набор в новые отделы)
- Используемые технологии (по требованиям к специалистам)
- Проблемы с текучкой кадров (частые повторные вакансии)

Использование OSINT-источников дает бизнесу конкурентное преимущество, позволяя реагировать на угрозы и устранять риски на ранних стадиях. Однако важно учитывать достоверность данных и соблюдать правовые нормы при сборе информации. Комплексный подход к анализу открытых данных помогает минимизировать риски и принимать обоснованные управленческие решения.

Пошаговая методика оценки рисков с помощью OSINT.

Методология поиска OSINT обеспечит структурированный и систематический подход к сбору, анализу и проверке общедоступных данных: [5]

1. Определите цели поиска.
2. Определите тип рисков
3. Подготовьте перечень источников информации.
4. Разработайте стратегию поиска.

После определения основных источников данных, которые будут использованы во время поиска, нужно указать стратегии поиска

5. Проведите сбор, оценку и анализ собранных данных.
6. Сформулируйте выводы и предложите рекомендации.

Правовые и этические аспекты применения OSINT в оценке рисков.

Несмотря на привлекательность применения методов OSINT для оценки рисков, эта деятельность требует строгого соблюдения правовых норм и этических принципов. На данный момент в РФ основным нормативно-правовым актом является Федеральный закон № 152-ФЗ "О персональных данных", который устанавливает четкие требования к сбору, хранению и обработке информации о физических лицах. А также для компаний, работающих с данными граждан стран ЕС, применяются и положения Общего регламента по защите данных (GDPR). [3]

Однако, ключевой проблемой правового аспекта неизменно остается определение границы между публичной и конфиденциальной информацией, потому что данные из социальных сетей и профессиональных платформ могут содержать и открытую информацию, и защищаемую законом о персональных данных. Особое внимание необходимо уделить анализу данных из незаконных утечек, так как их использование может противоречить положениям статей 128.1 и 137 УК РФ о клевете и нарушении неприкосновенности частной жизни.

Незаконными инструментами разведки могут быть [3]:

- Использование инсайдеров (подкуп сотрудников, свои “шпионы” в штате конкурента)
- Покупка еще не вышедших образцов.
- Прослушка телефонных звонков.
- Взлом баз данных (с закрытыми сведениями компании)
- Анализ отходов (например, отходов от шредера, покупка выброшенных архивов, старой документации).
- Поиск конфиденциальной информации о чужих сотрудниках или собственнике.
- Подкуп или шантаж чужого сотрудника.

К этическим аспектам применения OSINT относят необходимость соблюдения баланса между интересами компании и правами субъектов данных. Профессиональное сообщество выработало определенные принципы, включая минимизацию сбора персональных данных, отказ от

деанонимизации без веских оснований, обеспечение точности и объективности анализа.

Также у каждой отрасли рынка есть своя специфика, которая влияет на правовые рамки применения OSINT. Например, финансовые организации должны учитывать требования ЦБ РФ при проверке контрагентов, а IT-компании - ограничения на анализ открытого кода и данных из утечек. Для государственных предприятий действуют дополнительные ограничения, связанные с защитой государственной тайны.

Управление правовыми рисками при использовании OSINT требует знания внутренних регламентов, определяющих допустимые методы сбора и анализа данных, процедуры их хранения и уничтожения. Особое внимание уделяется документированию источников информации и методологии исследований, что может иметь критическое значение в случае судебных разбирательств.

Ниже представлены наиболее часто используемые инструменты OSINT (Таблица 1).

Таблица 1 – Инструменты OSINT

| Инструмент | Характеристика |
|---|---|
| **Maltego** | Инструмент для проведения расследований, который визуализирует связи между людьми, компаниями и точками онлайн-данных.<br>Подходит для расследования киберпреступлений и обнаружения мошенников. |
| **Intelligence X** | Поисковая система, которая находит и архивирует данные из открытых источников, даркнета и исторических записей.<br>Подходит для : глубокого поиска онлайн-данных, включая даркнет, утечки данных и исторический контент |
| **Crimewall по социальным ссылкам** | Инструмент для расследований, который собирает данные из более чем 500 открытых источников, включая социальные сети, приложения для обмена сообщениями, блокчейны и контент даркнета.<br>Подходит для : полного цикла расследований OSINT от сбора данных до окончательного отчета |

| | |
|---|---|
| **Shodan.io** | Поисковая система для устройств, подключенных к Интернету. Она охватывает все: от серверов и веб-камер до промышленных систем управления и устройств IoT. Лучше всего подходит для : обнаружения интернет-устройств и мониторинга безопасности сети |
| **SEON** | Инструмент для предотвращения мошенничества, который создает подробные цифровые следы пользователей, анализируя их адреса электронной почты, номера телефонов и IP-адреса. Лучше всего подходит для : анализа цифрового следа и предотвращения мошенничества с помощью OSINT |

Перспективы и рекомендации.

Юридические риски — это потенциальные угрозы, связанные с нарушением законов и нормативных актов, которые могут привести к финансовым потерям, репутационным ущербам или другим негативным последствиям для компании. Важно понимать, что юридические риски могут возникать в различных сферах деятельности компании и могут быть связаны как с внешними, так и с внутренними факторами.[6]

Разработка и внедрение внутренних политик и процедур

Создание четких внутренних политик и процедур помогает стандартизировать процессы и минимизировать вероятность возникновения юридических рисков.

Обучение сотрудников

Регулярное обучение сотрудников по вопросам соблюдения законодательства и внутренних политик компании помогает снизить вероятность возникновения юридических рисков. Это может включать проведение тренингов, семинаров и других образовательных мероприятий.

Внедрение системы управления рисками

Создание системы управления рисками позволяет систематически подходить к выявлению, оценке и минимизации юридических рисков. К этому относится использование специализированного программного обеспечения и других инструментов.

Страхование

Заключение договоров страхования может помочь минимизировать финансовые потери в случае наступления юридических рисков. Данный процесс может включать страхование ответственности директоров и должностных лиц, страхование профессиональной ответственности и другие виды страхования.

Понимание основных типов рисков, методов их идентификации и оценки, а также стратегий минимизации помогает снизить вероятность возникновения негативных последствий для компании. Регулярное

обучение, мониторинг изменений в законодательстве и внедрение систем управления рисками являются ключевыми элементами эффективного управления юридическими рисками. Важно также помнить, что управление юридическими рисками — это непрерывный процесс, который требует постоянного внимания и адаптации к изменяющимся условиям.

Заключение.

Данная статья демонстрирует яркий потенциал использования OSINT-техник в системе управления рисками для юридических лиц. В последние десятилетия благодаря цифровой трансформации исследование открытых источников информации становится незаменимым методом для выявления различных групп рисков.

Основные выводы исследования:

- OSINT обеспечивает комплексный подход к мониторингу рисков, сочетая оперативность получения данных и возможность их анализа.
- Работа с открытыми источниками требует четкой систематизации. Необходимо учитывать специфику бизнеса под конкретные бизнес-задачи.
- Эффективность OSINT напрямую зависит от используемых источников и соблюдения принципов верификации информации.

Особое внимание при применении OSINT всегда следует уделять соблюдению правовых и этических норм при применении OSINT-техник. Как показало исследование, юридические аспекты работы с открытыми данными требуют соблюдения законодательства о персональных данных, авторских правах и коммерческой тайне.

Благодаря анализу современных тенденций управления рисками с помощью OSINT выделяются такие перспективы как:

- автоматизация процессов сбора и анализа данных из открытых источников;
- внедрение искусственного интеллекта для обработки больших массивов данных;
- разработка стандартов применения OSINT для каждой отрасли;
- совершенствование нормативно-правовой базы, уточнение норм.

Таким образом, дальнейшее развитие использования OSINT в риск-менеджменте может способствовать повышению устойчивости компании в условиях динамично развивающегося миропорядка.

Список использованных источников:

1. Цифровая разведка OSINT и её роль в управлении бизнес-рисками [Электронный ресурс] Режим доступа: https://www.securitylab.ru/blog/personal/xiaomite-journal/353611.php.
2. Королева Д.С., Денисов А.А. Разработка метода сбора, анализа и мониторинга информации с целью выбора благонадежных участников сетевого предприятия в рамках контура конкурентной разведки // Инжиниринг предприятий и управление знаниями. 2023. С. 166-177.

3. Что такое конкурентная разведка: методы, этапы, основные источники информации. [Электронный ресурс] Режим доступа: https://spectrumdata.ru/blog/proverka-soiskatelya/chto-takoe-konkurentnaya-razvedka-metody-etapy-osnovnye-istochniki-informatsii/.

4. Горшкова С.А. Бизнес-разведка как составляющая обеспечения экономической безопасности бизнеса // Сборники конференций НИЦ Социосфера. – Пенза, 2020. – № 25. – С. 135-138.

5. Ларина Д.С. Бизнес-разведка как один из инструментов обеспечения успешного ведения бизнеса // Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения: материалы конференции. - СПб., 2019. - С. 518-522.

6. Д. Р. Хейс А. Б., Ф. Каппа, Исследование открытых данных для оценки рисков // Школа компьютерных наук и информационных систем Зайденберга - Нью-Йорк, 2018, С. 689-697.