Львов Константин Александрович

Магистрант кафедры информационной безопасности, НИУ МИЭТ

ПОДХОД К ФОРМИРОВАНИЮ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДРЯДЧИКОВ ОРГАНИЗАЦИЙ

В статье рассматривается проблема обеспечения информационной безопасности в процессе взаимодействия организаций с внешними подрядчиками и поставщиками. На основе анализа современных угроз, нормативных документов и практик управления рисками предложен комплексный подход к формированию требований по информационной безопасности подрядчиков. Применение предложенного подхода способствует снижению вероятности инцидентов, повышению прозрачности цепочек поставок и укреплению киберустойчивости бизнеса.

Ключевые слова: Информационная безопасность, Подрядчики, Цепочка поставок, Требования безопасности, Контроль поставщиков.

Рост атак через цепочки поставок стал одной из главных угроз современной кибербезопасности. Инциденты с компаниями SolarWinds, MOVEit и 3CX показали, что компрометация стороннего подрядчика способна парализовать деятельность даже крупнейших корпораций. Российская практика подтверждает тенденцию — увеличивается число атак на ИТ-интеграторов, разработчиков и сервисные компании.

Ключевая проблема заключается в отсутствии системного подхода к управлению безопасностью подрядчиков. Большинство организаций ограничиваются формальными мерами, не имея чёткой системы оценки и контроля.

Для реализации риск-ориентированного подхода подрядчиков целесообразно классифицировать по уровням критичности:

- Критичный уровень — подрядчики, от которых зависит функционирование ключевых бизнес-процессов (DevOps, инфраструктура);
- Высокий уровень риска — подрядчики с доступом к информационным ресурсам;
- Средний уровень — организации, имеющие ограниченный доступ;
- Низкий уровень — подрядчики, чья деятельность не влияет напрямую на безопасность компании.

Критериями оценки служат уровень доступа, влияние на непрерывность бизнеса и наличие регуляторных требований.

Анализ угроз показал, что наиболее типичными сценариями атак являются:

- внедрение вредоносных модулей в программные обновления;
- компрометация удалённого доступа и VPN;
- использование уязвимых библиотек open source;
- инсайдерская активность сотрудников подрядчика;
- подмена компонентов оборудования.

Методология ФСТЭК РФ и NIST IR 8272 рекомендуют сопоставлять модель угроз организации с моделью угроз подрядчика, включая возможных субподрядчиков. Такой подход позволяет выявить слабые звенья на ранних стадиях взаимодействия.

Предлагаемый подход включает три группы мер:

- Организационные — наличие ответственного за ИБ, сертификация, обучение сотрудников, отчётность об инцидентах;
- Технические — управление доступом по принципу наименьших привилегий, многофакторная аутентификация, шифрование данных, аудит и логирование, безопасная разработка (SAST/DAST, SLSA);

- Юридические — закрепление обязанностей по ИБ в договорах и SLA, подписание NDA, право на проведение аудита и пентестов.

Этот подход позволяет согласовать стандарты организации с практиками подрядчика и обеспечить единое пространство безопасности.

Эффективность подхода обеспечивается за счёт многоуровневого контроля:

1. Первичная оценка (анкетирование, сертификация, отчёты аудиторов).
2. Техническая верификация (пентесты, анализ кода, мониторинг активности).
3. Регулярный аудит — ревизия учётных записей, пересмотр требований, автоматизация проверки.

Компании, внедряющие такие процессы, по данным Positive Technologies (2024), сокращают вероятность инцидентов, связанных с подрядчиками, на 35–50%.

Организации, внедрившие данный подход, отмечают рост прозрачности цепочек поставок, улучшение взаимодействия с подрядчиками и снижение количества нарушений ИБ. Автоматизация мониторинга с применением систем IAM**,** PAM и GRC обеспечивает постоянную актуализацию рисков и повышает зрелость процессов управления безопасностью.

Практическую реализацию подхода можно разделить на этапы:

1. Этап инициации и инвентаризации

На первом этапе организация проводит инвентаризацию всех внешних контрагентов, включая технических партнёров, ИТ-интеграторов, провайдеров, а также подрядчиков, имеющих доступ к критическим бизнес-процессам. Формируется реестр подрядчиков с указанием:

- уровня доступа к корпоративной инфраструктуре и данным;
- используемых технологий и сервисов;

- наличия собственных мер защиты информации и сертификаций;
- истории инцидентов и репутации на рынке.

Реестр становится основой для последующего анализа рисков и выбора степени контроля для каждого подрядчика.

2. Этап анализа и классификации

После сбора данных подрядчики классифицируются по уровням критичности. Для этого используется балльная оценка на основе следующих параметров:

- наличие доступа к персональным данным и конфиденциальной информации;
- участие в критичных бизнес-процессах;
- техническая интеграция с внутренними системами;
- регуляторные требования, применимые к их деятельности.

Результаты оценки фиксируются в виде матрицы рисков, где для каждого уровня критичности устанавливается глубина проверки и перечень обязательных требований по ИБ.

3. Этап выстраивания требований

Для подрядчиков с высоким уровнем риска формируются расширенные требования, включающие:

- проведение регулярных внешних и внутренних аудитов безопасности;
- обязательное уведомление о выявленных уязвимостях и инцидентах;
- применение технологий шифрования и сегментации сетей при обмене данными;
- обязательное использование многофакторной аутентификации при доступе к корпоративным ресурсам.

Подрядчики со средним уровнем риска подлежат периодической проверке — раз в год или при изменениях инфраструктуры. Для низкорисковых подрядчиков устанавливаются минимальные организационные требования

(наличие базовых политик ИБ, антивирусной защиты, контроля доступа).

4. Этап проверки и мониторинга

Практическая реализация требует построения системы постоянного мониторинга и контроля. Эффективным решением является использование специализированных платформ класса TPRM (Third Party Risk Management), которые автоматизируют процесс анкетирования, проверки документов, формирования отчётов и анализа уязвимостей.
Для мониторинга технических рисков применяются:

- SIEM-системы для корреляции событий безопасности;
- DLP и UEBA для выявления подозрительных действий сотрудников подрядчиков;
- IDS/IPS для контроля сетевого взаимодействия.

Регулярный анализ логов и поведенческих аномалий позволяет выявлять подозрительные активности, связанные с доступом подрядчиков, и своевременно реагировать на инциденты.

5. Этап аудита и совершенствования

Минимум раз в год проводится пересмотр всех требований по ИБ и актуализация договорных условий. При выявлении новых рисков (например, появление уязвимостей в используемых библиотеках open source или изменениях в законодательстве) проводится внеплановая оценка подрядчиков.
Для критически важных поставщиков рекомендуется включать право на проведение внезапных аудитов или внешнего пентеста.

Список литературы

1. Рекомендации по минимизации возможных угроз безопасности информации при работе с подрядчиками [Электронный ресурс] //НКЦКИ. – URL: https://www.cert.gov.ru/materialy/ugrozy/653/ (дата обращения: 20.10.2025).

2. Утечки конфиденциальных данных из организаций – 1-е полугодие 2024: учебник для вузов [Электронный ресурс] // Positive Technologies. – URL: https://www.ptsecurity.com/research/analytics/utechki-dannyh-aktualnye-ugrozy-pervogo-polugodiya-2024-dlya-organizaczij (дата обращения: 20.10.2025).

3. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations [Электронный ресурс] // NIST SP 800-161 Rev.1. – URL: https://doi.org/10.6028/NIST.SP.800-161r1-upd1 (дата обращения: 20.10.2025).