УДК 004.056

Борзенков Александр Владимирович

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ), г. Москва, Россия,

КОМПРОМЕТАЦИЯ ПОДРЯДЧИКОВ КАК ВЕКТОР КИБЕРАТАК: АНАЛИЗ УГРОЗ И МЕРЫ ЗАЩИТЫ

Аннотация. Статья посвящена анализу компрометации подрядчиков и поставщиков услуг как самостоятельного вектора кибератак на организации. Рассмотрена типология атак через цепочку поставок программного обеспечения и ИТ-аутсорсинг, приведён анализ инцидентов SolarWinds и MOVEit/Cl0p, а также статистика Verizon DBIR, Positive Technologies и УЦСБ SOC, показывающая рост доли атак через доверенные каналы подрядчиков. На основе нормативной базы (ГОСТ Р ИСО/МЭК 27036, NIST SP 800-161, СТО БР ИББС-1.4-2018) предложена четырёхуровневая модель зрелости управления рисками подрядчиков и сформулированы практические рекомендации по снижению рисков цепочки поставок для организаций различного масштаба.

Ключевые слова: информационная безопасность, кибератака, цепочка поставок, компрометация подрядчиков, управление рисками, ИТ-аутсорсинг, критическая инфраструктура.

Borzenkov Aleksandr Vladimirovich

National Research Nuclear University MEPhI (NRNU MEPhI)

Moscow, Russia

Abstract. The article examines the compromise of contractors and service providers as an independent cyberattack vector against organizations. It analyzes the typology of software supply-chain and IT-outsourcing attacks, reviews the

SolarWinds and MOVEit/Cl0p incidents, and presents statistics from the Verizon DBIR, Positive Technologies, and UCSB SOC reports demonstrating the growing share of attacks conducted through trusted contractor channels. Based on the regulatory framework (GOST R ISO/IEC 27036, NIST SP 800-161, STO BR IBBS-1.4-2018), a four-level maturity model for third-party risk management is proposed, along with practical recommendations for reducing supply-chain risks for organizations of different scales.

Keywords: information security, cyberattack, supply chain, third-party compromise, risk management, IT outsourcing, critical infrastructure.

ВВЕДЕНИЕ

Цифровая трансформация бизнес-процессов сопровождается устойчивым ростом зависимости организаций от внешних подрядчиков — поставщиков программного обеспечения, интеграторов, провайдеров облачных услуг и managed service providers (MSP). Данная зависимость формирует протяжённую цепочку доверенных технологических связей, каждое звено которой потенциально расширяет поверхность атаки основной организации. Согласно данным ежегодного отчёта Verizon Data Breach Investigations Report за 2024 год, доля утечек данных, так или иначе связанных с третьей стороной — поставщиком услуг, разработчиком программного обеспечения или иным контрагентом, — достигла 15%, увеличившись на 68% по сравнению с показателем предыдущего отчётного периода [1]. Это делает компрометацию подрядчиков одним из наиболее динамично растущих векторов кибератак наряду с эксплуатацией уязвимостей и фишингом.

Практическая значимость проблемы обусловлена тем, что атака через подрядчика позволяет злоумышленнику обойти периметровые средства защиты целевой организации, используя легитимные учётные данные, доверенные каналы обновления программного обеспечения или предоставленный удалённый доступ. Формально в терминологии информационной безопасности под цепочкой поставок понимается

совокупность взаимосвязанных процессов производства, разработки, поставки и обслуживания программных и аппаратных средств, а под её компрометацией — внедрение вредоносного функционала либо получение несанкционированного доступа на любом из этапов данной цепочки [2]. Особенность подобных атак заключается в асимметрии ответственности: ущерб несёт конечная организация, тогда как точка первоначального проникновения зачастую находится вне зоны её прямого контроля.

Цель настоящей статьи — систематизировать типологию атак через компрометацию подрядчиков, проанализировать актуальную статистику и представительные инциденты, рассмотреть применимую нормативно-методическую базу и сформулировать практические рекомендации по управлению рисками цепочки поставок, включая авторскую модель зрелости соответствующих процессов.

1. ТИПОЛОГИЯ АТАК ЧЕРЕЗ КОМПРОМЕТАЫЦИЮ ПОДРЯДЧИКОВ

Атаки, реализуемые через подрядчиков, целесообразно разделить на четыре группы по объекту первичной компрометации.

Первая группа — атаки на цепочку поставок программного обеспечения (software supply chain attacks), при которых злоумышленник внедряет вредоносный код в легитимный продукт на этапе разработки, сборки или распространения обновлений. Показательным примером является инцидент SolarWinds (2019–2020 гг.), в ходе которого атакующие внедрили бэкдор SUNBURST в цепочку сборки платформы мониторинга Orion. Вредоносное обновление было автоматически установлено примерно у 18 000 клиентов компании, однако целенаправленное развитие атаки со сбором данных и закреплением в инфраструктуре было зафиксировано у существенно меньшего числа организаций — по разным оценкам, порядка 100–200, включая ряд федеральных агентств США и крупных технологических компаний [3]. Инцидент наглядно демонстрирует, что компрометация одного поставщика программного обеспечения способна одномоментно создать канал

проникновения в тысячи организаций, поскольку обновление распространялось через официальный, криптографически подписанный канал доставки.

Вторая группа — эксплуатация уязвимостей в программном обеспечении, используемом подрядчиками для оказания услуг конечным заказчикам (managed file transfer, RMM-системы, платформы удалённого администрирования). Характерный пример — атака группировки Cl0p на платформу передачи файлов MOVEit Transfer в мае–июне 2023 года с использованием ранее неизвестной SQL-инъекции (CVE-2023-34362), в результате которой на серверах MOVEit Transfer устанавливался веб-шелл LEMURLOOT, использовавшийся для хищения данных из базы данных приложения [4]. По данным независимого мониторинга инцидента, по состоянию на июнь 2024 года было подтверждено более 2773 пострадавших организаций и свыше 95,7 млн затронутых физических лиц, при этом значительная часть пострадавших организаций стала жертвой не прямой атаки на MOVEit, а компрометации своих подрядчиков и субподрядчиков, использовавших данную платформу [5]. Особенность данного класса атак — использование инфраструктуры, которой заказчик доверил обработку конфиденциальных данных, но над которой не имеет операционного контроля.

Третья группа — компрометация учётных данных и удалённого доступа ИТ- и ИБ-аутсорсеров (managed service providers), обслуживающих одновременно множество клиентов. Захват единой точки администрирования MSP предоставляет атакующему горизонтальный доступ ко всей клиентской базе провайдера без необходимости атаковать каждую организацию по отдельности.

Четвёртая группа — риски на уровне аппаратных поставок и субподрядчиков (компонентная база, прошивки, контрактное производство), при которых закладки или уязвимости внедряются до момента поставки оборудования конечному потребителю. Это наименее изученный, но

потенциально наиболее опасный класс угроз ввиду сложности верификации аппаратных цепочек поставок.

Общим для всех перечисленных сценариев является ключевой признак — использование установленных доверительных отношений в обход традиционных периметровых механизмов защиты.

2. ДИНАМИКА АТАК ЧЕРЕЗ ПОДРЯДЧИКОВ: ЭМПИРИЧЕСКИЙ АНАЛИЗ

Статистика последних лет подтверждает устойчивую тенденцию к росту доли атак, реализуемых через доверенные каналы подрядчиков. По данным исследования Positive Technologies «Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года», доля успешных атак, использующих доверительные отношения с контрагентами и подрядными организациями, за прошедший год выросла до 15%, при этом наиболее востребованной мишенью злоумышленников становится сама ИТ-отрасль, выступающая промежуточным звеном для проникновения в инфраструктуру конечных жертв [6]. Независимое исследование команды Threat Intelligence УЦСБ SOC по итогам 2025 года подтверждает данную тенденцию на более широкой выборке инцидентов: не менее 30% кибератак на российские организации в 2025 году были совершены через взлом подрядчиков, что позволило аналитикам отнести компрометацию цепочки поставок к числу ключевых киберугроз наступающего 2026 года [7]. Совпадение направленности выводов двух независимых исследовательских центров свидетельствует о системном, а не эпизодическом характере проблемы.

Сопоставление зарубежной и российской статистики позволяет сделать два вывода. Во-первых, рост доли атак через подрядчиков носит глобальный характер и не ограничивается отдельной юрисдикцией или отраслью — рост на 68% по методологии Verizon DBIR [1] и рост до 15–30% доли атак с использованием доверительных отношений по методологиям Positive Technologies [6] и УЦСБ SOC [7] представляют собой сопоставимые по направлению тенденции, несмотря на различие методик подсчёта. Во-вторых,

ИТ-отрасль и провайдеры аутсорсинговых услуг информационной безопасности сами становятся приоритетной целью атакующих именно в силу привилегированного доступа к инфраструктуре множества клиентов, что переводит вопрос защищённости подрядчика из зоны договорной ответственности в зону системного риска для всей обслуживаемой им клиентской экосистемы.

3. НОРМАТИВНО-МЕТОДИЧЕСКАЯ БАЗА УПРАВЛЕНИЯ РИСКАМИ ПОДРЯДЧИКОВ

Управление рисками информационной безопасности, связанными с подрядчиками, регламентируется рядом международных и национальных документов, различающихся по статусу и области применения.

Международный стандарт ИСО/МЭК 27036, действующий в Российской Федерации в виде серии ГОСТ Р ИСО/МЭК 27036 (части 1, 2, 3 и 4), определяет единый подход к управлению рисками информационной безопасности, возникающими при взаимодействии приобретающей стороны с поставщиками, включая поставщиков продукции и услуг ИКТ и облачных сервисов. Часть 1 стандарта задаёт понятийный аппарат и общие принципы, часть 2 — требования к системе управления взаимоотношениями с поставщиками, части 3 и 4 детализируют меры применительно к цепочке поставок ИКТ-продукции и облачным услугам соответственно [8].

Американский стандарт NIST SP 800-161 Rev. 1 «Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations», актуализированный в 2022 году во исполнение Указа Президента США № 14028, интегрирует управление киберрисками цепочки поставок (C-SCRM) в общий процесс риск-менеджмента организации на основе многоуровневого подхода — уровень организации, уровень бизнес-процессов и уровень отдельных систем — и содержит развёрнутый каталог мер защиты, согласованный с 20 семействами мер контроля из NIST SP 800-53. Документ применим как к государственным, так и к коммерческим организациям и охватывает полный жизненный цикл — от проектирования и разработки до

эксплуатации и вывода из эксплуатации [9]. В отличие от ГОСТ Р ИСО/МЭК 27036, ориентированного преимущественно на процессные требования, NIST SP 800-161 предлагает более детализированный практический инструментарий, включая типовой опросник для оценки зрелости поставщика (SCRM Assessment Scoping Questionnaire).

На отраслевом уровне в Российской Федерации действует стандарт Банка России СТО БР ИББС-1.4-2018 «Управление риском нарушения информационной безопасности при аутсорсинге», распространяющийся на кредитные и некредитные финансовые организации. Документ выделяет три модели взаимодействия с аутсорсерами — долгосрочную, среднесрочную и краткосрочную — и устанавливает требования к оценке рисков передаваемых на аутсорсинг функций, оценке возможностей поставщика услуг, содержанию договоров аутсорсинга и последующему мониторингу [10]. Существенное ограничение стандарта — рекомендательный характер его положений и отраслевая ограниченность применения финансовым сектором, что оставляет организации иных отраслей без обязательных к исполнению отраслевых требований к управлению рисками аутсорсинга.

Сопоставление рассмотренных документов показывает, что, несмотря на наличие развитой нормативно-методической базы, ни один из документов не носит универсального обязательного характера для всех отраслей российской экономики, а требования к субъектам критической информационной инфраструктуры регламентируют преимущественно защиту самой инфраструктуры, но не выстраивают системных требований к подрядчикам как самостоятельному объекту контроля.

4. ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ И МОДЕЛЬ ЗРЕЛОСТИ УПРАВЛЕНИЯ РИСКАМИ ПОДРЯДЧИКОВ

На основе проведённого анализа инцидентов и нормативной базы автором предлагается четырёхуровневая модель зрелости управления рисками подрядчиков (Third-Party Risk Management Maturity Model), позволяющая

организации оценить текущее состояние процессов и определить приоритетные направления развития.

Уровень 1 — «Ситуативный». Отбор подрядчиков осуществляется без формализованной оценки их состояния информационной безопасности; договоры не содержат требований к ИБ и порядка реагирования на инциденты; мониторинг действий подрядчика в инфраструктуре заказчика отсутствует. Данный уровень характерен для организаций малого бизнеса и создаёт максимальную экспозицию риска.

Уровень 2 — «Формализованный». Внедрена базовая процедура due diligence при выборе подрядчика (анкетирование, запрос сертификатов соответствия), в типовые договоры включены минимальные требования к защите информации, однако систематический контроль их исполнения не осуществляется, а доступ подрядчика к инфраструктуре не сегментирован.

Уровень 3 — «Управляемый». Организация применяет процессный подход в соответствии с положениями ГОСТ Р ИСО/МЭК 27036 либо аналогичного стандарта: проводится документированная оценка рисков для каждой категории подрядчиков, договоры содержат конкретные требования к уровню защищённости (SLA по ИБ, право на аудит), доступ подрядчиков предоставляется по принципу минимально необходимых привилегий (least privilege) с обязательной сегментацией сети и многофакторной аутентификацией, действия подрядчика в инфраструктуре регистрируются и анализируются средствами SIEM.

Уровень 4 — «Оптимизируемый». Управление рисками подрядчиков интегрировано в общую систему управления киберрисками организации по модели, сопоставимой с NIST SP 800-161: применяется непрерывный мониторинг состояния защищённости подрядчиков (в том числе с использованием внешних рейтинговых сервисов), в договоры включены требования к совместному тестированию плана реагирования на инциденты, регулярно проводится независимый аудит критически значимых подрядчиков,

а остаточные риски частично передаются посредством страхования киберрисков.

Практические рекомендации, вытекающие из представленной модели, включают следующие меры. Во-первых, категоризация подрядчиков по уровню критичности предоставляемого доступа и обрабатываемых данных с дифференцированными требованиями безопасности для каждой категории. Во-вторых, обязательное включение в договоры конкретных, измеримых требований к информационной безопасности и права заказчика на проведение аудита или получение результатов независимой оценки. В-третьих, реализация принципа наименьших привилегий и сетевой сегментации для любого удалённого доступа подрядчика, включая обязательное использование многофакторной аутентификации и ограничение времени действия предоставленных учётных данных. В-четвёртых, непрерывный мониторинг активности подрядчиков в инфраструктуре заказчика с фиксацией отклонений от типового поведения. В-пятых, разработка и регулярное тестирование совместного плана реагирования на инциденты, учитывающего сценарии компрометации через подрядчика. Наконец, регулярный, не реже одного раза в год, пересмотр перечня критически значимых подрядчиков и актуализация требований к ним с учётом изменения ландшафта угроз.

ЗАКЛЮЧЕНИЕ

Проведённый анализ показывает, что компрометация подрядчиков представляет собой самостоятельный и динамично растущий вектор кибератак, использующий доверительные отношения для обхода традиционных периметровых средств защиты. Инциденты SolarWinds и MOVEit/Cl0p продемонстрировали, что компрометация единственного поставщика программного обеспечения способна затронуть тысячи организаций одновременно, а статистика Verizon DBIR, Positive Technologies и УЦСБ SOC подтверждает устойчивый рост доли подобных атак как в мировом, так и в российском контексте. Существующая нормативно-методическая база — ГОСТ Р ИСО/МЭК 27036, NIST SP 800-161 и отраслевой

СТО БР ИББС-1.4-2018 — формирует необходимый концептуальный фундамент, однако носит преимущественно рекомендательный либо отраслевой характер и не обеспечивает универсального обязательного регулирования вопросов безопасности цепочки поставок для организаций всех отраслей.

Предложенная в статье четырёхуровневая модель зрелости управления рисками подрядчиков может быть использована организациями в качестве практического инструмента самооценки и планирования развития процессов управления рисками цепочки поставок. Направлением дальнейших исследований представляется разработка количественных метрик оценки зрелости для каждого уровня модели и эмпирическая верификация предложенного подхода на выборке организаций различных отраслей экономики.

Литература:

1. Verizon Business. 2024 Data Breach Investigations Report [Электронный ресурс]. - URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (дата обращения: 18.07.2026).

2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. - М.: Горячая линия - Телеком, 2004. - 280 с. - ISBN 5-93517-197-X.

3. Rudis, B. SolarWinds SUNBURST Backdoor Supply Chain Attack: What You Need to Know [Электронный ресурс] // Rapid7 Blog. - 2020. - URL: https://www.rapid7.com/blog/post/2020/12/14/solarwinds-sunburst-backdoor-supply-chain-attack-what-you-need-to-know/ (дата обращения: 18.07.2026).

4. StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability: Cybersecurity Advisory AA23-158A [Электронный ресурс] / Cybersecurity and Infrastructure Security Agency, Federal Bureau of

Investigation. - Washington, 2023. - URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (дата обращения: 18.07.2026).

5. Simas, Z. Unpacking the MOVEit Breach: Statistics and Analysis [Электронный ресурс] // Emsisoft Blog. - 2023 (обновлено 28.06.2024). - URL: https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (дата обращения: 18.07.2026).

6. Актуальные киберугрозы: IV квартал 2024 года - I квартал 2025 года [Электронный ресурс] // Positive Technologies. - 2025. - URL: https://ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 18.07.2026).

7. Ключевые тренды киберугроз 2025 и прогнозы на 2026 год [Электронный ресурс] / Команда Threat Intelligence УЦСБ SOC, ООО «УЦСБ». - Екатеринбург, 2026. - URL: https://soc.ussc.ru/soc-report-2025 (дата обращения: 18.07.2026).

8. ГОСТ Р ИСО/МЭК 27036-1-2021. Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия. - Введ. 2021-11-30. - М.: Стандартинформ, 2021. - 20 с.

9. NIST SP 800-161r1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations [Электронный ресурс] / J. Boyens [и др.]; National Institute of Standards and Technology. - Gaithersburg, MD, 2022. - URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf (дата обращения: 18.07.2026).

10. СТО БР ИББС-1.4-2018. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге / Банк России. - Введ. 2018-07-01. - М., 2018.