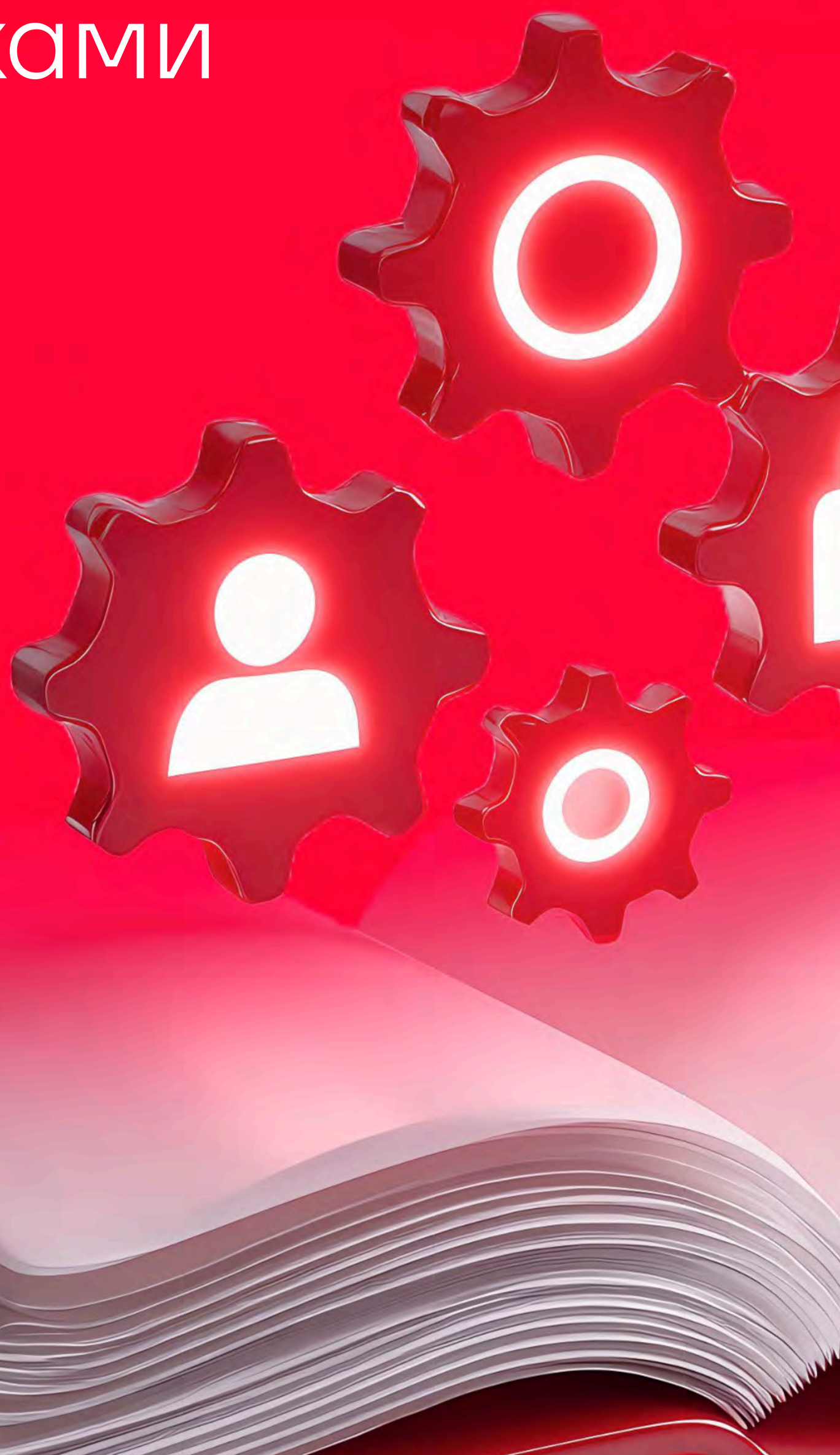
ИНДИД

Гайд

по работе с подрядчиками



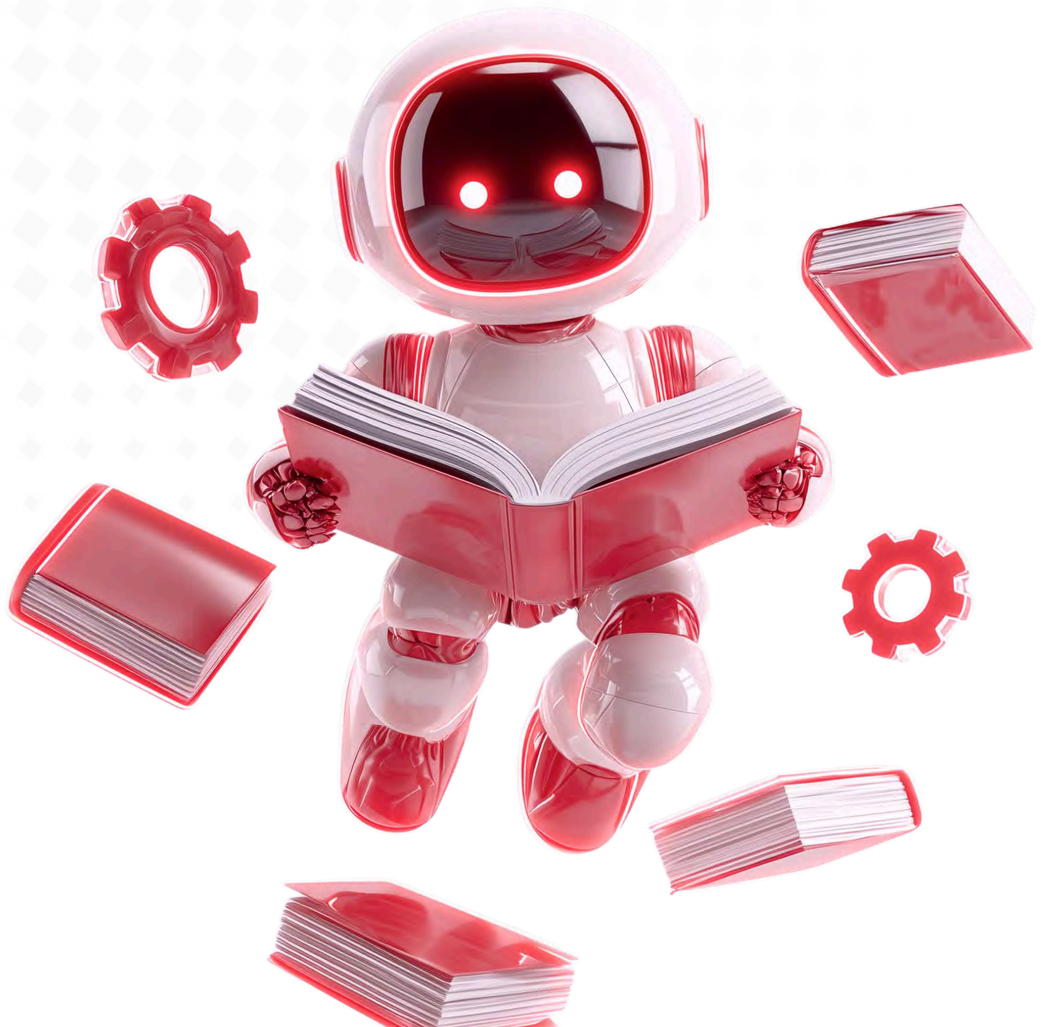
Гайд

Защищаем доступ к ИТ-инфраструктуре

Сегодня атаки через поставщиков и партнеров становятся одним из ключевых киберрисков для организаций любого масштаба и отрасли. В России их число стремительно растет: по данным НКЦКИ за последний год именно компрометация через доверенные каналы с подрядчиками стала наиболее распространенной угрозой для бизнеса.

Это связано с тем, что современные компании активно внедряют и развивают множество ИТ-сервисов, все чаще привлекая внешних разработчиков и поставщиков ПО. Для совместной работы им приходится предоставлять подрядчикам удаленный доступ к своей инфраструктуре. С одной стороны, это упрощает взаимодействие и экономит ресурсы, но с другой — создает серьезные угрозы безопасности. Наличие пользователей с расширенными или неконтролируемыми правами увеличивает риски несанкционированного доступа к ИТ-инфраструктуре с последующей реализацией цепочки атак.

Чтобы помочь компаниям защитить доступ к инфраструктуре, компания «Индид» разработала гайд по организации безопасного удаленного доступа внешних специалистов. В нем собраны практические рекомендации — от настройки политик доступа до предоставления прав и прекращения полномочий. Следуя этим шагам, вы сможете обеспечить безопасное и удобное взаимодействие с подрядчиками, повысить прозрачность процессов и значительно снизить риски и инцидентов в ИТ-инфраструктуре.



Ключевые риски

По данным исследования Positive Technologies, в 2024 г. доля атак, в ходе которых злоумышленники проникали в инфраструктуру организации через компанию-подрядчика, выросла до 15% (в 2021–2023 гг. подобные инциденты отмечались только эпизодически). Компрометация учетных данных одной компании открывает путь к системам множества ее клиентов. Человеческий фактор, слабая парольная политика, отсутствие разграничения прав и надежной аутентификации остаются ключевыми уязвимостями корпоративной безопасности.

Ниже приведены главные угрозы, возникающие при предоставлении внешним пользователям доступа к корпоративной инфраструктуре:

Избыточные права доступа

Компании нередко выдают подрядчикам расширенные или полные административные права «для удобства», а после завершения работ не ограничивают их вовремя или вовсе не удаляют учетные записи (УЗ).

Риски: подрядчики сохраняют возможность выполнять несанкционированные действия даже после окончания договора.

Таким образом, злоумышленник, получивший доступ к скомпрометированной УЗ, может собирать данные, изучать сеть и готовить атаку на ценные активы. Административные права позволяют ему создавать скрытые УЗ, изменять права сервисных аккаунтов или устанавливать легитимное ПО с автозапуском, обеспечивая себе постоянный доступ после удаления основной УЗ подрядчика.

Невыполнение аудита подключений

Во многих компаниях не ведутся полные журналы аутентификации и не фиксируются действия пользователей (кто, когда и что выполнял).

Риски: без аудита сложно или невозможно своевременно расследовать инциденты и восстановить ход событий. В результате действия злоумышленников, особенно во время рабочего дня, могут выглядеть как обычная работа администраторов.

Использование небезопасных каналов связи

Подрядчики нередко подключаются к ИТ-ресурсам по протоколам RDP/VNC без должного шифрования, используют общие пароли или допускают подключения по RDP из открытых сетей.

Риски: учетные данные легко перехватить или подобрать, что создает высокий риск несанкционированного доступа к инфраструктуре.

Передача данных неразрешенными способами

Подрядчики могут умышленно или по ошибке скопировать конфиденциальную информацию на внешние носители или сторонние облачные ресурсы.

Риски: подобные действия ведут к утечкам данных, нарушению законодательства и договорных обязательств.

Выполнение работы с помощью личных устройств

Некоторые подрядчики работают с личных устройств, неподконтрольных заказчику и потенциально зараженных вредоносным ПО.

Риски: такие устройства могут стать источником серьезных угроз для корпоративной инфраструктуры. Например, программы-вымогатели (ransomware), попавшие в сеть, способны зашифровать общие диски и нарушить работу компании.

Отсутствие сетевой сегментации

Доступ подрядчиков часто не ограничен отдельным сегментом сети, что позволяет им перемещаться между сегментами.

Риски: злоумышленник может осуществить атаку путем латерального перемещения и повышения прав доступа, получив контроль над критически важными ресурсами, включая системы резервного копирования и производственную сеть.

Доступ без временных ограничений

Иногда подрядчикам предоставляется круглосуточный доступ без контроля рабочих периодов и автоматического отзыва прав.

Риски: злоумышленники могут использовать легитимные учетные записи вне установленного времени, включая период после завершения работ. Если учетная запись не отключена, ее данные могут утечь и попасть на теневые форумы. Злоумышленники, входящие в состав APT-группировок, часто действуют ночью или в выходные, когда администраторы неактивны: проводят разведку, похищают данные или устанавливают вредоносное ПО, маскируя атаку под действия подрядчика.

Выводы

При недостаточном контроле информационной безопасности при работе с подрядчиками формируется неконтролируемая среда доступа: создаются многочисленные учетные записи с разными правами, отсутствует актуальный реестр и контроль их предоставления. В результате невозможно определить, какие учетные записи действительны, а какие подлежат удалению.
Это свидетельствует о низкой зрелости процессов управления доступом и повышает риски для информационной безопасности, операционной деятельности и соблюдения нормативных требований.

Варианты атак и их последствия

Чтобы получить несанкционированный доступ к ИТ-инфраструктуре компании, злоумышленники нередко эксплуатируют уязвимости в программном обеспечении и конфигурациях систем подрядчиков, используя слабые места. Последствия таких проникновений могут включать утечку конфиденциальных данных, простои сервисов и компрометацию доверенных каналов.

Основные виды атак на подрядчиков, проводимые APT-группировками:

- **Атака на цепочку поставок (Supply Chain Attack):** злоумышленник компрометирует ИТ-поставщика, внедряя бэкдор в продукт, который тот разрабатывает или обслуживает. В результате под угрозой оказываются все клиенты организации.
- **Атака типа «человек посередине» (Man-in-the-Middle, MitM):** злоумышленник «отправляет» кэш протокола разрешения адресов ARP или подменяет DNS, чтобы перенаправить трафик подрядчика через свою машину. Это позволяет ему перехватывать команды.
- **Вредоносное ПО (инфостилеры):** в последние годы активно применяется массовая установка специализированных программ с целью кражи любой полезной информации. Риск растет, если сотрудники организаций выполняют рабочие задачи с помощью личных устройств.

В 2024 г. был обнаружен взлом систем американской компании Snowflake, которая специализируется на облачном анализе данных. Предполагается, что злоумышленники заразили инфостилером ПК одного из сотрудников этой фирмы. В результате оказалась скомпрометирована персональная информация сотен миллионов частных лиц, пользующихся услугами компаний — клиентов Snowflake. В частности, подтверждена кража данных клиентов Santander Bank и Ticketmaster.

Гайд / Варианты атак и их последствия

При отсутствии реальных мер контроля организация рискует столкнуться с серьезными последствиями, в числе которых:

- **утечка конфиденциальной информации** (финансовых отчетов, персональных данных клиентов, коммерческих секретов);
- **проникновение злоумышленников в инфраструктуру** (компрометация учетной записи подрядчика позволяет APT-группировкам получить доступ в сеть компании);
- **саботаж** (удаление информации, отключение сервисов, подмена конфигураций);
- **нарушение законодательства** (152-ФЗ, 187-ФЗ, нормативных актов Банка России) и, как следствие, получение штрафов от регулирующих органов;
- **репутационные потери** (утечки данных, получившие огласку, могут существенно снизить доверие клиентов).

Наиболее распространенными последствиями кибератак на организации в России остаются утечки конфиденциальных данных и сбои в работе компаний. По сравнению с 2023 годом и первой половиной 2024-го доля успешных атак с утечкой информации увеличилась с 44% до 56%, а доля успешных атак, приводивших к нарушению деятельности компаний, увеличилась с 37% до 40%. Чаще всего похищались служебные документы, содержащие коммерческую тайну (30%), учетные записи (24%), а также персональные данные клиентов и сотрудников (17%).

Меры безопасности

Для предотвращения подобных угроз организациям необходимо пересмотреть бизнес-процессы и внедрить контроль за подрядчиками. Только технических мер становится недостаточно — требуется изменение подходов к работе.
Из-за возможных ограниченных ресурсов трансформация может занять время, поэтому план действий следует реализовывать поэтапно. Его рекомендуется начинать с внедрения организационных мер и процессов, регламентирующих получение прав доступа.

Организационные меры

Опыт глобальных ИТ-компаний показывает, что стратегию безопасности следует реализовывать комплексно — в рамках единой политики удаленного доступа подрядчиков и третьих лиц, основанной на принципе нулевого доверия (Zero Trust). В ней необходимо четко определить:

- кто и при каких условиях получает доступ к ИТ-ресурсам;
- срок его действия;
- используемые инструменты;
- порядок проведения аудита.

Политика удаленного доступа также должна включать следующие положения:

Условия предоставления доступа

Удаленный доступ разрешается только при выполнении всех требований:

- подписаны соглашения о конфиденциальности (NDA) и согласие с политикой безопасности;
- подписан и вступил в силу контракт или дано рабочее задание, в котором обозначена необходимость удаленного доступа;
- запрос на доступ одобрен ответственным за проект/систему сотрудником компании.

Аутентификация

При подключении обязательно используется многофакторная аутентификация (MFA).

Двухфакторная аутентификация (2FA) — наиболее распространенный вариант MFA, обеспечивающий дополнительный уровень защиты и значительно снижающий риск компрометации учетной записи. Даже если злоумышленник смог получить логин или пароль от учетной записи, пройти еще один фактор аутентификации ему будет крайне сложно.

С этой целью клиенты компании «Индид» применяют Indeed Access Manager (Indeed AM) — систему для многофакторной аутентификации и централизованного управления доступом, которая обеспечивает строгий контроль и единую процедуру проверки подлинности пользователей при доступе к корпоративным информационным ресурсам. Решение имеет модульную архитектуру, что позволяет легко адаптировать его под нужды компании и поддерживает множество методов аутентификации, в том числе технологию Single Sign-On, использование одноразовых паролей и push-уведомлений.

Разграничение и контроль прав доступа

Согласно политике нулевого доверия (Zero Trust), доступ предоставляется только в том объеме, который необходим для выполнения конкретных задач, указанных в контракте. Права доступа («только чтение», «изменение», «администратор» и т. д.) назначаются явным образом и регулярно пересматриваются. По умолчанию подрядчикам запрещен доступ ко всем ресурсам.

Список действий, запрещенных подрядчику

Включает любые операции, способные нарушить безопасность, целостность или стабильность ИТ-инфраструктуры компании. Например, запрещается устанавливать несанкционированное ПО на устройства, используемые для доступа.

Для реализации принципов Zero Trust мы предлагаем использовать решение Indeed Privileged Access Manager (Indeed PAM). Продукт обеспечивает контроль и управление привилегированным доступом, микросегментацию сети с точным разграничением прав, шифрование трафика и непрерывный мониторинг сессий для выявления аномалий. Перед предоставлением доступа система проводит проверку и авторизацию пользователей и приложений, применяет многофакторную аутентификацию и позволяет ограничивать действия, включая выполнение команд и передачу файлов (SSH, RDP). При обнаружении подозрительной активности администратор может оперативно деактивировать пользователя.

Защищенный виртуальный рабочий стол (VDI)

Предусматриваются два варианта использования устройств для выполнения рабочих задач. Предпочтительно использование защищенного виртуального рабочего стола (VDI), управляемого ИТ-службой заказчика. Данные при этом не покидают корпоративный периметр. Альтернативный вариант — это работа с собственных устройств подрядчиков при соблюдении требований: утвержденный антивирус, актуальные обновления, шифрование диска, включенный межсетевой экран, запрет на использование устройства в личных целях.

Правила мониторинга и аудита деятельности подрядчиков

Для предотвращения несанкционированного доступа, утечек данных, нарушения политик безопасности, а также для обеспечения прозрачности действий подрядчиков компаниям необходимо установить правила мониторинга и аудита их деятельности в своих информационных системах. Под наблюдением должны находиться:

- доступ к файлам, базам данных, внутренним ресурсам;
- операции с конфиденциальной информацией;
- использование учетных записей и привилегий;
- сетевые подключения и передача данных;
- применение внешних носителей и устройств.

Порядок действий при возникновении инцидентов

Для обеспечения устойчивой защиты информационных систем от несанкционированного доступа и последующей компрометации, необходимо установить и согласовать порядок действий и перечень оперативных мер, принимаемых для быстрого реагирования на инциденты.

Правила прекращения доступа и аудит учетных записей подрядчиков

Права доступа подрядчика автоматически аннулируются в день завершения контракта. Если сотрудничество заканчивается досрочно, то менеджер проекта должен уведомить об этом ИТ-службу для отзыва прав доступа. Также следует проводить регулярный аудит всех активных учетных записей подрядчиков с целью удаления устаревших.

Регламент получения прав доступа

Для обеспечения контролируемого и безопасного доступа подрядчиков к информационным системам компании устанавливается следующий порядок и процессы его получения:

Предоставление доступа только по заявке — время доступа и функции подрядчика строго ограничиваются.

Обязательное уведомление — подрядчик заранее сообщает, когда и зачем он будет подключаться.

Многоэтапная проверка: права доступа утверждают сначала владелец ИТ-системы, к которой планирует подключиться подрядчик, а далее — внутренний заказчик (тот, в чьих интересах проводятся изменения) и сотрудник центра мониторинга (если возникнут проблемы, то центр мониторинга сможет четко указать, какие работы выполняются в данный момент).

Технические меры

Для защиты корпоративных ресурсов и минимизации рисков несанкционированного доступа устанавливаются следующие технические меры, обеспечивающие безопасное подключение и работу подрядчиков.

Микросегментация сети

Для повышения уровня защиты разрабатываются отдельные политики безопасности для каждого сегмента сети. Они определяют допустимые подключения, разрешенные протоколы и действия пользователей. Такая изоляция предотвращает перемещение злоумышленника внутри сети даже при компрометации одной машины.

Подрядчики получают доступ только к необходимому сегменту без возможности сканировать сеть или перемещаться между сегментами. Использование ограничивается строго определенными протоколами.

Indeed PAM обеспечивает управление привилегированным доступом на основе групп и подразделений, позволяет распределять администраторов и пользователей по ролям, выдавать доступ по расписанию, предоставлять одноразовые разрешения на подключение и автоматически завершать неактивные сессии по тайм-ауту.

Парольная политика в серверном сегменте

В серверном сегменте применяется усиленная парольная политика, направленная на предотвращение несанкционированного доступа и повышение киберустойчивости ИТ- инфраструктуры.

Все учетные записи должны иметь сложные пароли, соответствующие корпоративным требованиям по длине, уникальности и сложности. Для защиты от подбора паролей реализуется механизм блокировки — доступ временно приостанавливается, например, на 30 минут после пяти неудачных попыток входа за две минуты.

Использование паролей по умолчанию и общих учетных записей запрещено. Пароли необходимо регулярно менять, а их обновление осуществлять с помощью специализированных программных средств. Для хранения и управления учетными данными используется локальный корпоративный менеджер паролей (on-prem), который может инициировать смену паролей, если это невозможно сделать штатными средствами. При этом доступ к серверам необходимо осуществлять только по зашифрованным каналам, следует избегать вспользования незащищенных протоколов. Все события входа в систему подлежат аудиту и мониторингу, что позволяет выявлять подозрительную активность — попытки входа в нерабочее время, с неизвестных IP-адресов или частые ошибки аутентификации.

Indeed PAM обеспечивает автоматическую ротацию паролей без их раскрытия подрядчикам. Этот механизм служит дополнительной защитой на случай попыток брутфорс-атак при нарушении микросегментации. Система хранит пароли в зашифрованном виде и позволяет автоматически их изменять по расписанию, выдавая временные разрешения на подключение без раскрытия паролей. Функционал Indeed PAM поддерживает создание паролей по заданным правилам, обеспечивая соответствие их требованиям безопасности. Пароли служебных учетных записей хранятся в защищенном хранилище и подставляются в приложения и скрипты автоматически, без участия пользователей. Дополнительно реализована возможность добавить второй фактор для аутентификации даже в таких системах, архитектура которых не предусматривает многофакторную аутентификацию.

Сеть с «нулевым доверием» и VPN с многофакторной аутентификацией

Использование сети с «нулевым доверием» (Zero Trust Network Access, ZTNA) в сочетании с VPN и многофакторной аутентификацией (MFA) обеспечивает высокий уровень безопасности при удаленном доступе. Применение VPN между подрядчиком и сегментом DMZ, содержащим общедоступные сервисы и изолирующим их от внутренних ресурсов, предотвращает перехват данных. ZTNA блокирует подключение до прохождения второго фактора аутентификации, а также позволяет ограничить доступ по заданному перечню IP-адресов, минимизируя риск несанкционированного входа.

Внедрение решения для управления привилегированным доступом (PAM)

Настройка системы управления привилегированным доступом (PAM) обеспечивает безопасный контроль действий пользователей с повышенными правами. Доступ к ресурсам осуществляется исключительно через систему PAM с обязательным применением второго фактора аутентификации. Решение контролирует узлы, протоколы и время подключения, выдает временные пароли или одноразовые токены, а все действия фиксируются посредством видео- и текстовой записи сессий.

Мониторинг и применение SIEM-систем:

Мониторинг и применение SIEM-систем позволяют оперативно выявлять аномальную активность. Настраиваются автоматические оповещения о подозрительных действиях, таких как подключения в нерабочее время, запрещенные операции через PAM, массовое удаление файлов или изменение конфигураций.

В частности, Indeed PAM обеспечивает полный аудит действий пользователей: записывает и воспроизводит сессии, логирует события и сохраняет артефакты в централизованном хранилище, независимом от локальных ресурсов. Это позволяет анализировать действия сотрудников и подрядчиков как в реальном времени, так и ретроспективно — для оперативного контроля и расследования инцидентов. Кроме того, система поддерживает отправку событий в любые SIEM-системы без дополнительных коннекторов, используя стандартные форматы логов CEF и LEEF.

Чек-лист по внедрению

Шаг 1. Аудит

- [ ] Составить список всех подрядчиков, у которых есть доступ.
- [ ] Проверить, какие используются учетные записи и каналы.
- [ ] Выявить и заблокировать учетные записи бывших подрядчиков и непонятные аккаунты существующих.
- [ ] Проанализировать архитектуру сети.
- [ ] Проанализировать парольную политику.

Шаг 2. Сегментация и изоляция

При необходимости изменить конфигурацию сети, обеспечив максимально эффективную сегментацию.

Шаг 3. Выбор и внедрение инструментов ИБ

- [ ] При необходимости внедрить и настроить MFA и VPN, выделить сегмент DMZ (Demilitarized Zone) для подключения подрядчиков.
- [ ] Выбрать и внедрить систему контроля привилегированного доступа (PAM).

Шаг 4. Изменение регламентов и описаний процессов

- [ ] Утвердить новую политику удаленного доступа.
- [ ] Внести в договоры с подрядчиками требования безопасности.
- [ ] Определить роли и зоны ответственности (например, менеджера проекта/заказчика, ИТ-службы, корпоративной службы безопасности, центра мониторинга), составить четкие описания этих ролей и зон.
- [ ] Прописать процедуры предоставления и отзыва прав доступа, а также процедуры контроля со стороны центра мониторинга.
- [ ] Определить порядок взаимодействия в нештатных ситуациях.
- [ ] Определить регламент завершения проекта и возврата/уничтожения данных.

Шаг 5. Настройка средств контроля

- [ ] Включить запись сессий.
- [ ] Настроить систему SIEM/мониторинг ключевых событий.
- [ ] Обеспечить ежеквартальный (или более частый) аудит прав доступа.
- [ ] При необходимости внедрить **систему IdM** для автоматизации управления учетными записями. Это позволит автоматизировать онбординг подрядчиков, периодический аудит их прав и отключение (при завершении контракта или при признаках взлома подрядчика). **Например, Octopus IdM.**

Шаг 6. Обучение и культура

- [x] Обучить внутренних сотрудников правильному взаимодействию с подрядчиками.
- [x] Разъяснить подрядчикам правила подключения и последствия их нарушения.

Выводы

Для обеспечения информационной безопасности важно не только внедрять современные меры и средства защиты, но и объяснять сотрудникам их значение и преимущества. Новые решения должны быть максимально удобны и понятны пользователям — как специалистам ИБ, так и администраторам. При этом повышать требования к безопасности следует постепенно: чрезмерные ограничения часто приводят к обходным действиям и новым рискам.

Эффективный контроль удаленного доступа подрядчиков требует централизованной, управляемой системы. Ключевую роль играют организационные меры, подкрепленные современными продуктами, такими как решения классов PAM, IAM и IdM, средствами микросегментации и мониторинга. Комплексный подход, включающий оптимизацию регламентов, внедрение решений, обучение и постоянный контроль, позволяет закрыть все уязвимости — от утечек данных до несанкционированного перемещения по сети.

ИНДИД

Контакты

Вы готовы начать?

Не откладывайте безопасность на завтра — защитите свой бизнес уже сегодня.

Свяжитесь с нами, и наши эксперты помогут с формированием плана улучшений по внедрению решений для контроля и управления доступом.

indeed-company.ru

sales@indeed-company.ru

8 800 333-09-06