JET SECURITY TEAM

АТАКИ НА ПОДРЯДЧИКОВ

ЭКСПЛУАТАЦИЯ ДОВЕРИЯ

ИССЛЕДОВАНИЕ

ОГЛАВЛЕНИЕ

КЛЮЧЕВЫЕ ВЫВОДЫ И ЦИФРЫ

80%
компаний используют защитные меры в отношении подрядчиков/поставщиков услуг, аналогичные удаленным работникам

ЛИШЬ 20%
определяют набор мер, исходя из специфики взаимодействия и профиля риска поставщика

МЕНЕЕ 10%
проводят мероприятия по оценке уровня ИБ поставщика услуг. Оценка проводится в основном с использованием опросных листов и зачастую носит формальный характер — не влияет на дальнейшее решение о выборе поставщика или архитектуры подключения к ресурсам компании

«CASTLE AND MOAT»
(«крепость и ров», также известна как «защита периметра») до сих пор одна из самых часто встречающихся моделей построения ИБ. Фокус на защите периметра относительно эффективен против внешнего злоумышленника, однако после успешной компрометации подрядчика в такой инфраструктуре атакующий имеет полный «карт-бланш»

38%
компаний для обмена большими файлами со сторонними компаниями используют внешние бесплатные сервисы. При этом работник – инициатор обмена, как правило, самостоятельно определяет требования к безопасности, руководствуясь принципами скорости и удобства

85%
компаний, где ПО сопровождал подрядчик, не имели стратегии «выхода» в случае ухода поставщика с рынка или передачи сервиса другому игроку

В 3 РАЗА
за последние годы вырос спрос на решения, связанные с сокращением риска компрометации данных при внешнем взаимодействии. Так, например, спрос на решения класса PIM/PAM, по нашим данным, вырос в 3,2 раза с 2019 года.

АННОТАЦИЯ

Исследование посвящено анализу проблем и рисков, связанных с атаками через сторонние организации, когда злоумышленники атакуют целевую компанию не напрямую, а через ее доверенных партнеров, поставщиков или подрядчиков. Такие атаки также называют «эксплуатацией доверия» и «атаками на цепочку поставок».

Цели исследования:

- Обозначить основные риски на разных этапах взаимодействия участников цепочки поставок
- Обозначить ключевые проблемы российских компаний в данной области
- Оценить готовность компаний к противодействию таким атакам
- Дать рекомендации по управлению рисками взаимодействия с партнерами и подрядчиками

Основу исследования составили:

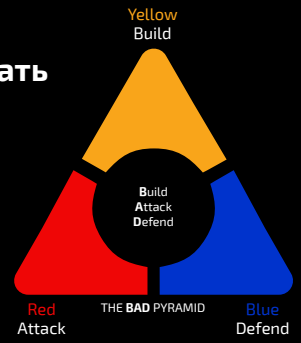
- Данные, полученные в ходе реализации проектов по аудиту информационной безопасности, тестированию на проникновение
- Результаты мониторинга и реагирования на инциденты в рамках оказания сервисов SOC со стороны команды мониторинга Jet CSIRT
- Результаты расследования компьютерных инцидентов со стороны экспертов по форензике
- Аналитика, полученная по результатам работы группы мониторинга внешних цифровых рисков

КОНЦЕПЦИЯ И МЕТОДОЛОГИЯ

Исследование основывается на концепции пирамиды кибербезопасности BAD Pyramid (Build, Attack, Defend)[1].

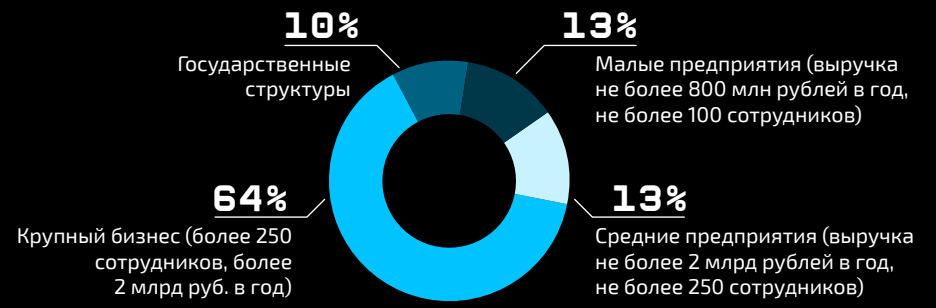
Данный принцип предлагает рассматривать объект оценки со стороны трех команд:

- Команд, проектирующих и строящих системы защиты (Yellow Team)
- Команд атакующих (Red Team)
- Команд защитников (Blue Team)



Такой подход позволяет обеспечить всесторонний взгляд на объект исследования и сформировать комплексную оценку проблемы.

В отчет также вошли результаты опросов ключевых заказчиков АО «Инфосистемы Джет» и внешних опросов профильной аудитории. В опросах приняло участие более 50 компаний, большинство которых (64%) представители крупного бизнеса, а также малые и средние предприятия и компании государственного сектора.



[1]https://danielmiessler.com/study/red-blue-purple-teams/

ВВЕДЕНИЕ

Согласно отчетам аналитических компаний[2], риск эксплуатации доверия (Supply Chain / Third-party Risk) входит в ТОП-5 наиболее критичных и вероятных среди других типов операционных рисков за последние три года, а рост количества атак на цепочки поставок, по разным источникам, составляет от 300% и более[3]. Риск эксплуатации доверия необходимо рассматривать в контексте двух основных категорий поставщиков:

- Деловые партнеры и подрядчики
- Поставщики программного обеспечения

Атаки на подрядчиков и поставщиков ПО схожи, но имеют разные способы реализации и специфичные методы защиты. Матрица MITRE ATT&CK[4] выделяет две основные техники, связанные с эксплуатацией доверия:

- T1199 — атака на доверительные отношения (Trusted Relationship)
- T1195 — компрометация цепочки поставок (Supply Chain Compromise)

В отчете подробно рассматриваются атаки типа Trusted Relationship, реализуемые, как правило, через компрометацию сторонних компаний. Злоумышленники сначала попадают в инфраструктуру к незащищенному поставщику, а затем продвигаются далее для получения доступа к более крупной жертве.

Безопасность цепочки поставок программного обеспечения (Software Supply Chain Compromise) является важным аспектом более широкой темы — безопасности приложений, которая требует отдельного исследования и намеренно осталась за скобками.

[2]Отчет форума передового опыта по операционным рискам (OpRisk Company) за 2023 год, BCI Horizon Scan Report 2022
[3]Software Supply Chain Attacks: 2021 in Review,Aqua. CrowdStrike's Global Security Attitude Survey, 2021.
[4]Проект от американской копрорации MITRE. Является де-факто стандартом для классификации и описания действий атакующих и содержит около 200 различных техник или способов проведения атак.

ИСТОРИЧЕСКАЯ СПРАВКА

Публичные инциденты в 2022-2023 годы еще раз доказывают растущее влияние атак эксплуатации доверия на бизнес: простои систем, денежные потери, ущерб для репутации.
Вот лишь некоторые громкие инциденты:

01. 2022 Атака на крупного поставщика услуг аутентификации Okta с целью использовать их доступ к клиентским инфраструктурам. Компания Okta подтвердила инцидент и сообщила, что атака затронула более 350 организаций-клиентов.

09.2022 Злоумышленники проникли в инфраструктуру чат-провайдера Comm100 и подменили их установщик, внедрив в него вредоносный код. Злоумышленники получили доступ к данным клиентов компании, которые использовали зараженную версию ПО Comm100. Количество потенциальных клиентов, которые могли скачать вредоносное ПО — более 15 000 организаций.

10.2022 Государственная железная дорога в Дании была остановлена на несколько часов из-за кибератаки на стороннего поставщика ИТ-услуг — компанию Supeo.

03.2023 Атака на разработчика VoIP-решений 3CX. Десктопный клиент 3CXDesktopApp был скомпрометирован и использовался для распространения вредоносного ПО среди клиентов компании. Потенциальное количество атакованных — более 600 000 компаний по всему миру, включая American Express, Coca-Cola, BMW, Toyota, IKEA и др.

04.2023 ИнфоТеКС, утечка архива с 60 912 учетными записями пользователей по вине подрядчика, ответственного за разработку нового сайта.

JET SECURITY TRUSTED RELATIONSHIP FRAMEWORK

В 2022 году в центре информационной безопасности «Инфосистемы Джет» был разработан собственный фреймворк — Jet Security Trusted Relationship Framework (JSTRF). Результаты экспертных аудитов ИБ, опыт работы с широкой линейкой средств защиты различных классов, а также собственная пентест-лаборатория помогли сформулировать основные проблемы, с которыми сталкиваются компании, и определить, что позволяет киберпреступникам успешно совершать атаки на эксплуатацию доверия.

Фреймворк представляет собой концепцию управления рисками безопасности третьих лиц и учитывает три ключевых этапа жизненного цикла взаимодействия с подрядчиками.

В рамках исследования перечисленные этапы были сгруппированы в три укрупненных блока:

1. Инициализация взаимодействия
2. Управление взаимоотношением
3. Прекращение работы

Далее каждый из этапов подробно рассматривается с использованием методологии BAD Pyramid в контексте контролей безопасности, входящих в состав фреймворка JSTRF.

ИНИЦИАЛИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ 1

УПРАВЛЕНИЕ ВЗАИМООТНОШЕНИЕМ 2

ПРЕКРАЩЕНИЕ РАБОТЫ 3

ПЛАНИРОВАНИЕ И ИНИЦИАЛИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ

Планирование взаимоотношений с поставщиком

Оценка целесообразности привлечения третьих лиц

- Определение перечня критичных функций/сервисов и ограничений при привлечении третьих лиц
- Анализ/независимая оценка целесообразности взаимодействия

Методология

- Политики взаимодействия с поставщиками в рамках модели жизненного цикла
- Политики выбора третьих лиц и оценки их уровня безопасности
- Ресурсная модель управления процессом и RACI
- Политики безопасного использования сервисов и ресурсов для работников /поставщиков
- Управление рисками поставщиков в политике закупок/управлении проектами

Набор защитных мер

- Типовые архитектуры ИБ при взаимодействии
- Профили рисков поставщиков

Управление рисками

- Оценка рисков взаимодействия
- Метрики эффективности и контрольные показатели уровня риска

Управление инцидентами

- Сценарии/планы реагирования на инциденты с поставщиком (утечки и пр.)

Оценка и выбор поставщиков

Оценка «зрелости ИБ» поставщика

- Независимый аудит третьей стороной
- Оценка цифровых рисков (DRP)
- Оценка по формальным контролям/ собственный аудит

Оценка потенциала поставщика

- Оценка квалификации и ресурсного обеспечения
- Оценка репутации и финансового положения

Оценка ограничений при взаимодействии

- Оценка регуляторных ограничений
- Оценка зависимости деятельности поставщика от субподрядчиков
- Кадровая безопасность сотрудников поставщика
- Оценка лицензионных и иных ограничений

Непрерывность бизнес–процессов

- Поддержка перечня альтернативных поставщиков
- Мониторинг уровня концентрации функций у поставщиков
- План поддержания процессов отработки отказов (BCM/DRP), стратегия «выхода»

Закрепление обязанностей сторон

Соглашение о взаимодействии

- Разграничение ответственности и управление обязательствами сторон в области ИБ
- Учет регуляторных требований при взаимодействии
- Совместное управление инцидентами ИБ
- Совместное использование интеллектуальной собственности, коммерческой и иных видов тайн
- Штрафные санкции за нарушение мер безопасности
- Управление персональными обязательствами (Personal NDA)
- Обеспечение непрерывности и восстановления функций (SLA)
- Аспекты ИБ и условия привлечения субподрядчиков
- Управление персональными обязательствами (Personal NDA)

Учет поставщиков

- Ведение расширенного реестра поставщиков и перечня атрибутов

Инициализация взаимодействия

Организация безопасного доступа к ресурсам

- Безопасность удаленных подключений (VPN/СКЗИ))
- Соответствие конечных устройств требованиям ИБ
- Безопасность оперативной коммуникации
- Безопасный терминальный доступ
- Защита межсистемных интеграций/API
- Организация безопасного аварийного доступа
- Безопасный обмен файлами
- Безопасность совместной проектной области
- Управление привилегированным доступом
- Тестирование на безопасность ИТ-компонент поставщика

Управление инцидентами

- Интеграция сервисов поставщика в мониторинг

Процессы ИБ*

- Обучение персонала правилам безопасного взаимодействия
- Управление и контроль доступа
- Управление архитектурой ИБ
- Управление изменениями конфигураций
- Ознакомление поставщика с требованиями ИБ/тренинги
- Управление обновлениями
- Управление уязвимостями
- Безопасность физического доступа

Защита инфраструктуры и данных*

- Защита корпоративных данных
- Защита от утечек данных
- Маркировка данных и управление метками конфиденциальности
- Маскирование данных/ обезличивание тестовых сред
- Шифрование данных
- Мультифакторная аутентификация
- Антивирусная защита
- Микросегментация
- Защита от майнинга
- Контроль подключения устройств
- IPS/IDS

УПРАВЛЕНИЕ ВЗАИМООТНОШЕНИЕМ

Управление взаимоотношением

Контроль соответствия

- Оценка цифровых рисков (DRP)
- Отчетность поставщика

Управление риском

- Регистрация событий риска взаимодействия
- Мониторинг уровня концентрации функций у поставщиков
- Мониторинг контрольных показателей уровня риска и метрик
- Сводная отчетность о качестве и безопасности взаимодействия

Контроль защищенности совместной инфраструктуры риском

- Управление уязвимостями
- Тестирование на проникновение (в т.ч. по модели «нелояльный поставщик»)

Обеспечение непрерывности

- Мониторинг соблюдения установленных значений SLA
- Тестирование планов BCP, зависящих от услуг поставщика
- Резервное копирование данных и защита РК

Управление инцидентами

- Сбор событий безопасности
- Реагирование на инциденты ИБ

ПРЕКРАЩЕНИЕ РАБОТЫ

Прекращение работы

- Поддержка перечня активов, находящихся у поставщика
- Контроль уничтожения данных на стороне поставщика
- Контроль возврата активов поставщиком
- Контроль прекращения эксплуатации/возврата информационных систем

*** Конечный перечень процессов и технических мер определяется по результатам адаптации профиля риска поставщика**

ЭТАП 1
«ИНИЦИАЛИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ» ОБЩИЕ ВЫВОДЫ

Специфика этапа: между компанией и поставщиком услуг инициируется взаимодействие по следующим направлениям:

- правовое — закрепление договорных обязательств;
- информационное — предоставление доступа в инфраструктуру и обмен данными;
- организационное — следование поставщиком корпоративным правилам безопасности.

В соответствии с JSTRF **укрупненные** задачи компании на данном этапе сводятся к следующему:

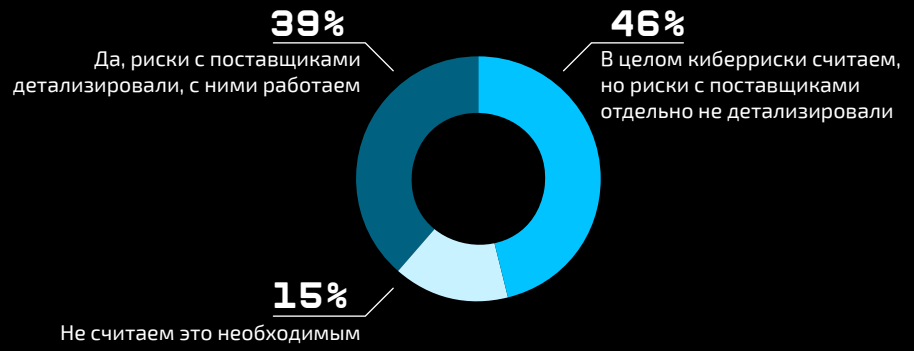
- оценить целесообразность привлечения поставщиков для оказания услуг;
- определить «правила игры»: политики взаимодействия с поставщиками и процедуры управления риском;
- оценить возможности поставщика услуг обеспечить необходимый уровень ИБ и отсеять явно небезопасные компании;
- определить меры, соизмеримые с уровнем риска поставщика, обеспечить безопасную буферную зону для работы с подрядчиком;
- проработать юридические и организационно-технические вопросы совместного использования информации и ресурсов.

Результаты опроса

Чтобы оценить, как компании управляют рисками ИБ на данном этапе, мы попросили ответить на следующие вопросы:

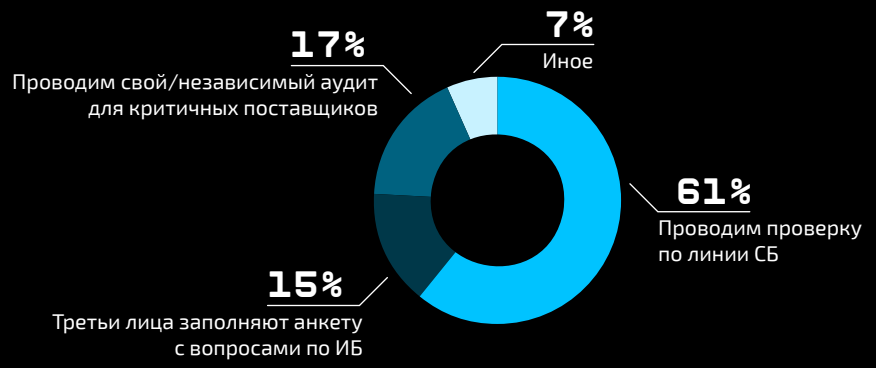
1. Оцениваете ли вы киберриски, связанные со взаимодействием с поставщиками?
2. Формализован ли процесс безопасного взаимодействия с поставщиками?
3. Оцениваете ли вы уровень риска ИБ поставщиков до начала взаимодействия?
4. Что вы включаете в договор с поставщиками?

Согласно полученной обратной связи, подавляющее большинство рассматривает киберриски взаимодействия с поставщиками в совокупности с другими рисками без детализации, при этом значительная часть участников опроса не считает такую оценку необходимой. Детальная проработка киберрисков, связанных с поставщиками, осуществляется в основном крупными компаниями и госсектором.



Процедуры взаимодействия с поставщиками формализованы в виде элементарных требований по безопасной передаче информации у большинства респондентов. Специфичные политики, учитывающие особенности каждого этапа жизненного цикла взаимодействия, отмечены менее чем у 20% опрошенных.
В основном киберриски поставщика оцениваются проверкой по линии СБ, реже – с использованием опросников с формальными критериями.

При этом почти все участники опроса стараются обезопасить себя в рамках договора включением в него как стандартного NDA, так и минимальных требований по ИБ для поставщиков.



Что мы наблюдаем

Непрозрачность существующих взаимоотношений (с кем и как строится взаимодействие) и применение практики «один подход для всех» являются ключевыми проблемами, наблюдаемыми у большинства исследованных компаний на данном этапе:

- В большинстве случаев в компаниях отсутствует формализация политик управления рисками взаимодействия с третьими лицами, что было также отмечено большинством опрошенных. Такая практика обусловлена в целом низким уровнем зрелости процессов риск-менеджмента ИБ в российских компаниях, где оценка рисков часто носит формальный характер или не проводится.

- Мероприятия по оценке поставщика по линии ИБ проводят менее 10% компаний, что коррелирует с результатами опроса. Оценка проводится в основном с использованием опросных листов и зачастую носит формальный характер — не влияет на дальнейшее решение о выборе поставщика или архитектуры подключения к ресурсам компании. При этом привлечение консалтинговых организаций или использование сервисов для проведения оценки поставщиков наблюдалось только у 3% компаний, во всех случаях такие сервисы предоставлялись зарубежной управляющей компанией.

- Шаблоны соглашений о неразглашении (NDA) с поставщиками услуг в большинстве компаний содержат общие требования по безопасности. Только в 5% компаний были отмечены понятные правила безопасного использования корпоративных ресурсов, процедуры эскалации в рамках инцидента, возможные штрафные санкции за нарушение требований ИБ.

По нашему мнению, ключевые причины данных проблем заключаются в следующем:

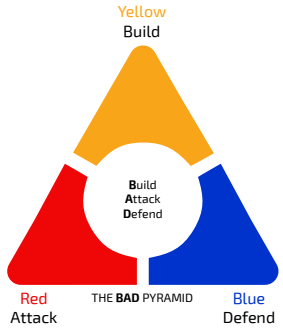
- Российский рынок продуктов по управлению рисками поставщиков развит слабо, несмотря на то, что на на мировом рынке представлено большое количество как отдельных решений (UpGuard Vendor Risk, Panorays Security Passport и др.), так и специальных модулей в составе GRC-решений.

- Оценка квалификации, опыта и репутации поставщиков требует много времени и соответствующих компетенций, обычно выполняется в ручном режиме на основе анкет. Сервисы скоринга на основе данных киберразведки только начинают развиваться.

- Отсутствуют стандартизированные российские фреймворки (по аналогии с SIG Questionnaire, CAIQ и др.), которые ввели бы единую «линейку» и дали возможность компаниям демонстрировать внешним партнерам свой уровень ИБ для упрощения процедуры выбора и управления рисками взаимодействия.

- Неустоявшаяся практика использования ограничений, связанных с уровнем ИБ поставщика, в политике закупок.

BAD PYRAMID



Распространенные проблемы данного этапа, чаще всего приводящие к инцидентам:

- Небезопасные архитектуры взаимодействия с поставщиком
- Небрежное управление учетными записями
- Обмен файлами с использованием небезопасных методов
- Размытая зона ответственности за инцидент: как юридическая, так и фактическая

Yellow Team

Наиболее часто наблюдаемые в рамках проектов небезопасные схемы подключения поставщиков:

- клиентский VPN без второго фактора;
- публикация службы RDP-сервера в сеть интернет без сертификатов;
- использование несконфигурированных служб RDS для публикации приложений.

В рамках выбора «как удобно» и «как безопасно» с перевесом побеждает первое, при этом зачастую компанию от взлома отделяет **всего три клика мышкой.**

В рамках аудита был обнаружен опубликованный в интернете сервер с RDP. Попытка авторизации со случайными УЗ прошла успешно из-за отключенного NLA. Учетная запись администратора была защищена вторым фактором, вот только токен был подключен к рабочей станции, а пароль к учетной записи содержался в подсказке.

Наиболее частые замечания по результатам аудитов — проблемы с управлением учетными данными. Пароли от корпоративных ресурсов для доступа поставщиков чаще всего мы обнаруживаем в системах HelpDesk (при оформлении заявки на создание УЗ), в корпоративной почте, сервисах коммуникации (Slack, Teams и пр.).

Red Team

В более чем 50% случаев внешние сервисы (корпоративная почта, портал) компании эксплуатируются без второго фактора, поэтому успешный фишинг приводит к их компрометации. В отличие от собственных сотрудников, для которых можно регулярно проводить awareness-обучение, сотрудники подрядчика чаще **попадаются на фишинг.**

Распространенным ресурсом для обмена данными с поставщиком выступают «буферные» папки на FTP, VDR и внешних витринах данных. Взлом учетной записи поставщика от таких сервисов гарантированно приводит к компрометации данных компании (**часто — крайне чувствительных**), которые в беспорядке годами хранятся в таких папках.

Так в рамках одного из тестирований на проникновение из-под УЗ поставщика была доступна стратегия вывода нового бренда на рынок и сопутствующая документация, «временно» сохраненная в папке Shared.

Blue Team

В рамках сервиса мониторинга внешних цифровых рисков мы системно анализируем DarkNet и Телеграм-каналы злоумышленников. Анализ теневых ресурсов за первый квартал 2023 года показал рост популярности атак через подрядчиков среди злоумышленников.
Атакующие выбирают наиболее крупных поставщиков ИТ-услуг, чаще всего это разработчики ПО. Затем проводят для этих компаний сканирование внешнего периметра с целью поиска уязвимостей, после чего выбирают в первую очередь те компании, которые имеют наиболее критичные уязвимости, для которых существуют готовые эксплойты.
Проэксплуатировав уязвимости и оказавшись внутри периметра, атакующие пытаются проникнуть во внутренний периметр заказчика, если не получается, то просто шантажируют IT-компанию.

В одном из Телеграм-каналов были обнаружены скриншоты доступов к ресурсам крупной компании. Анализ контекста переписки показал, что взлом произошел по вине подрядчика, автоматизирующего процессы операционной деятельности. Оперативно локализовав скомпрометированный сегмент, удалось остановить атаку.

ЭТАП 2
«УПРАВЛЕНИЕ ВЗАИМООТНОШЕНИЕМ» ОБЩИЕ ВЫВОДЫ

Специфика этапа: необходимый уровень информационной безопасности в ходе работы с поставщиком поддерживается за счет следующих процессов:

- поддержание непрерывности бизнес-процессов, зависящих от поставщика услуг;
- управление инцидентами ИБ, возникающими во время оказания услуг;
- мониторинг уровня риска и контроль соблюдения установленных требований ИБ поставщиком.

В соответствии с JSTRF **укрупненные** задачи компании на данном этапе сводятся к следующему:

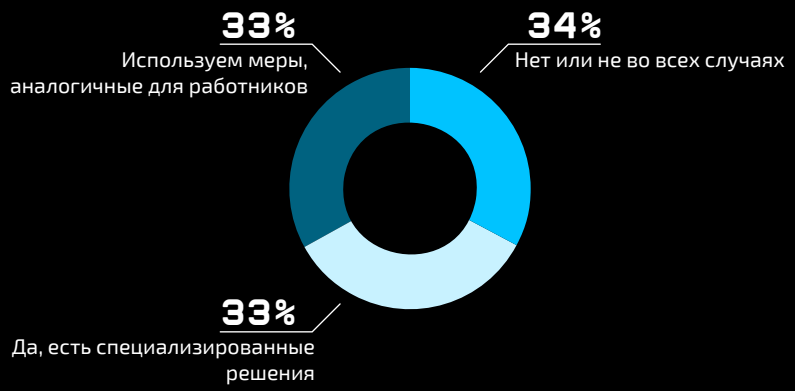
- защитить сегмент инфраструктуры, предназначенный для совместной работы;
- обеспечить непрерывный мониторинг активности поставщиков, в том числе уровня их безопасности, с использованием данных киберразведки;
- обеспечить техническую защиту прав собственности на технологии и информацию компании;
- проработать механизмы восстановления в случае сбоев;
- обучать персонал, вовлеченный в процесс взаимодействия, аспектам информационной безопасности.

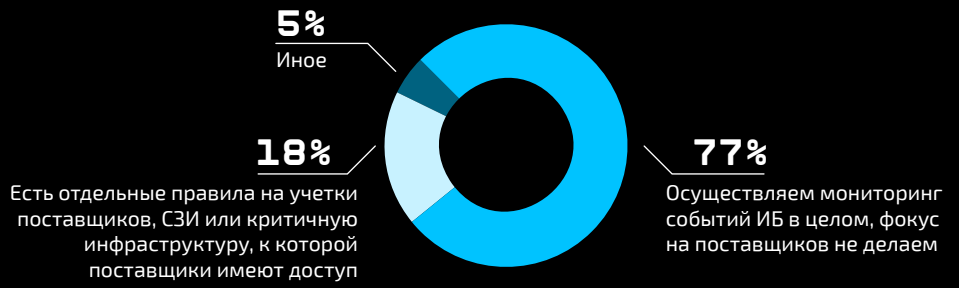
Результаты опроса

Чтобы оценить, как компании управляют рисками ИБ на данном этапе, мы попросили ответить на следующие вопросы:

1. Применяете ли вы какие-либо дополнительные технические меры защиты при работе с поставщиками?
2. Какие меры по мониторингу событий ИБ, связанных с поставщиками, реализованы?

Значительная часть участников опроса не использует какие-либо дополнительные контрольные меры применительно к поставщикам либо применяет те же меры, что и для сотрудников компании. При этом только 18% опрошенных компаний задумались о мониторинге событий ИБ, связанных с поставщиком (отдельные правила выявления).





Что мы наблюдаем

«Castle and Moat» (или «крепость и ров», также известна как «защита периметра») до сих пор одна из самых часто встречаемых моделей построения ИБ. Фокус на защите периметра относительно эффективен против внешнего злоумышленника, однако после успешной компрометации подрядчика в такой инфраструктуре атакующий имеет полный «карт-бланш»:

- В 80% компаний защитные меры в отношении поставщиков являются аналогичными удаленным работникам, только в 20% набор мер определялся исходя из специфики взаимодействия и профиля поставщика, что также подтверждают результаты опроса.

- Несмотря на изменение парадигмы построения архитектуры безопасности в сторону моделей нулевого доверия («никогда не доверяй, всегда проверяй»), в отношении поставщиков доминирует модель «один раз проверяй — всегда доверяй». Практика последующей переоценки/мониторинга риска поставщика (после первичного «отбора») практически не распространена в российских компаниях. Только 5% компаний, использующих сервисы по выявлению цифровых рисков, добавляли в область анализа (помимо своего периметра) внешних поставщиков.

- Реагирование на атаки со стороны поставщиков услуг в 90% компаний осуществляется по общим схемам (playbooks), практика постановки учетных записей критичных поставщиков на мониторинг слабо распространена. Административная активность подрядчика является сложной для анализа и требует отдельных правил: для выявления признаков компрометации нужен анализ отклонений от стандартной модели поведения. Как правило, компании не разделяют типы административных учетных записей для мониторинга, хотя такая информация помогла бы быстрее принять меры по реагированию.

- В 38% компаний для обмена большими файлами с внешними подрядчиками используются внешние бесплатные сервисы. При этом работник – инициатор обмена, как правило, самостоятельно определяет требования к безопасности, руководствуясь принципами быстроты и удобства.

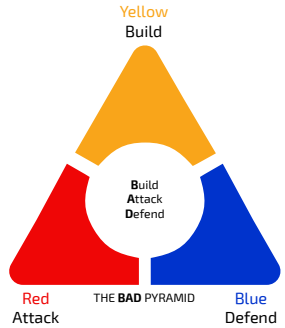
По нашему мнению, ключевые причины данных проблем заключаются в следующем:

- Существующие регуляторные требования в отношении рисков аутсорсинга/привлечения поставщиков разработаны в большей части для участников финансового рынка, и они не содержат единых подходов к управлению подобными рисками и понятных инструкций «что надо делать». В международной практике вопрос управления поставщиками услуг проработан более детально.

- Отсутствие регулирования привлечения отдельными участниками рынка поставщиков услуг (для участников финансового рынка такое регулирование поэтапно вводится Банком России).

- Недофинансирование сферы ИБ. Выделяемые бюджеты в основном тратятся на «средства первой необходимости» — лицензии, ФОТ, обновление решений. Мы практически не наблюдаем выделения финансирования на проверку уровня ИБ текущих поставщиков или специализированные решения по управлению риском взаимодействия.

BAD PYRAMID



Распространенные проблемы данного этапа, чаще всего приводящие к инцидентам:

- Избыточные полномочия учетных записей поставщиков
- Игнорирование базовых требований ИБ при разработке продуктов
- Слабая сетевая изоляция сегмента инфраструктуры, предназначенного для совместного взаимодействия
- Использование продуктивных данных в тестовых системах

Yellow Team

После включения поставщика в цепочку поставок и получения административных полномочий такие третьи лица **часто живут своей жизнью**, самостоятельно назначая себе права или создавая более удобные способы администрирования.

На одном из проектов по внедрению PIM был обнаружен теневой канал доступа поставщика в сеть компании. Безопасная схема администрирования с MFA была неудобна, поэтому подрядчик опубликовал в сеть интернет свой терминальный сервер с RDP и словарным паролем.

Из-за операционной нагрузки сотрудники кибербезопасности не могут (а часто и не хотят) погружаться в ИТ-процессы и проекты, поэтому случаи, когда **компания просто не управляет целыми кусками своей инфраструктуры**, не редкость. В этом случае на проектах по аудиту и внедрению приходится опрашивать сотрудников подрядчика, так как штатный персонал не знает паролей ни от root, ни от административных УЗ приложения.

Red Team

В случаях, когда отсутствуют минимальные требования к ИБ подрядчика, его сотрудники могут использовать для своих УЗ простые словарные пароли.

В рамках web-тестирования системы управления персоналом, внедряемой поставщиком, помимо уникального пароля все пользователи имели еще один — технический. Сбор логинов на сайте + пять цифр пароля — и доступ к системе бухгалтерии у злоумышленника в кармане.

«Забывчивость» — еще одна распространенная привычка поставщиков. Вот наш ТОП:

- забытые тестовые скрипты в веб-приложении с возможностью выполнения команд в ОС;
- забытые резервные копии приложений и служебные страницы веб-приложений с уязвимостями;
- забытый или оставленный намеренно функционал, используемый в тестовых целях, например, для обхода стандартной процедуры аутентификации в панель администратора.

Blue Team

Время с момента появления в открытом доступе скомпрометированных паролей до последующей атаки сократилось до нескольких часов. Чувствительные данные чаще всего оседают в публичных репозиториях кода, которые мы систематически мониторим.

Один из последних кейсов: нашей командой был обнаружен факт публикации кода во внешний репозиторий, содержащего пароли администратора в открытом виде. После оповещения компании и сброса паролей мы детектировали попытки аутентификации с использованием скомпрометированной учетной записи. С момента утечки на тот момент прошло не более четырех часов.

ЭТАП 3
«ПРЕКРАЩЕНИЕ РАБОТЫ» ОБЩИЕ ВЫВОДЫ

Специфика этапа: обеспечение безопасности во время прекращения взаимодействия:

- изъятие и уничтожение критичной информации для предотвращения ее несанкционированного распространения;
- возврат реквизитов доступа, ограничение доступа к ресурсам.

В соответствии с JSTRF **укрупненные** задачи компании на данном этапе сводятся к следующему:

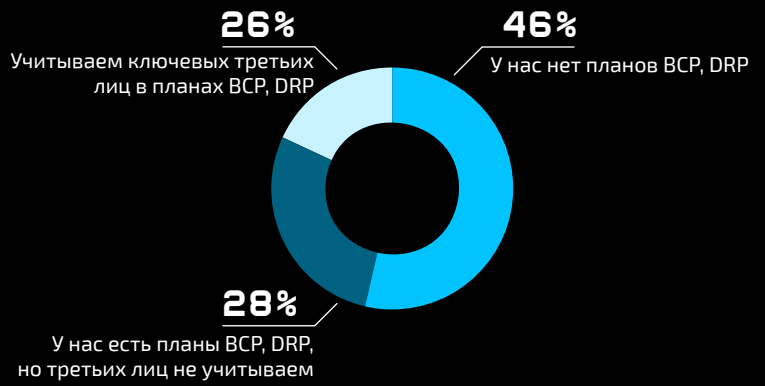
- выбрать и согласовать активы, которые будут возвращены компании/поставщику или гарантированно уничтожены;
- обеспечить безопасное прекращение эксплуатации/возврата информационных систем и блокировку доступов поставщиков в инфраструктуру компании;
- активировать планы непрерывности бизнеса в случае внезапного прекращения сервиса/услуги поставщиком.

Результаты опроса

Чтобы оценить, как компании управляют рисками ИБ на данном этапе, мы попросили ответить на следующий вопрос:

Учитывают ли планы обеспечения непрерывности и восстановления (BCP, DRP) ключевых поставщиков услуг?

Подавляющее число компаний не проводит оценку влияния ИТ-поставщиков на непрерывность деятельности организации. В случае инцидента, связанного с поставщиком, только 18% опрошенных компаний, преимущественно крупного бизнеса, смогут оперативно предпринять действия по восстановлению согласно планам обеспечения непрерывности и восстановления.



Что мы наблюдаем

Отказ от исполнения договора может быть инициирован на любом этапе жизненного цикла и часто бывает незапланированным. Успех продолжения выполнения бизнес-функций своими силами (или передачи их иному поставщику) во многом зависит от зрелых процессов непрерывности бизнеса и управления активами. Когда такие процессы зрелые — с высокой вероятностью будет обеспечена доступность критичных сервисов, а лишние артефакты не останутся в инфраструктуре и ничего «не забудется» на стороне поставщика:

- В большинстве компаний, где ПО сопровождал подрядчик, отсутствовала стратегия «выхода» в случае ухода поставщика с рынка или передачи сервиса другому игроку. При этом многими компаниями была отмечена технологическая зависимость от поставщиков услуг, в основном обусловленная ограниченным числом поставщиков, оказывающих необходимые услуги.

- Самый распространенный в NDA и вместе с этим самый игнорируемый способ передачи и возврата активов — оформление акта приема-передачи. Ввиду объемов передаваемой информации и постоянной коммуникации такой метод является архаизмом и используется только для передачи КТ или других документов с грифом. При этом требование по уничтожению корпоративных данных на стороне поставщика — редко встречаемая практика, обычно в NDA включаются только стандартные требования не разглашать конфиденциальную информацию в течение определенного периода времени.

- Незаблокированные учетные записи поставщиков - «призраков» мы наблюдаем практически на каждом проекте.

По нашему мнению, ключевыми причинами данных проблем стали:

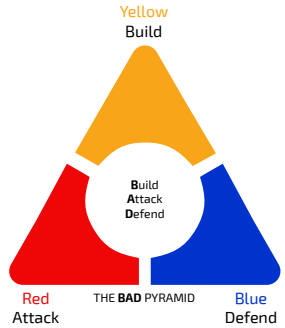
- Низкий уровень зрелости процессов непрерывности бизнеса в российских компаниях, рассмотрение рисков непрерывности исключительно с технической стороны. Планы непрерывности бизнеса практически никогда не учитывают зависимости от критичных поставщиков.

- Отсутствие до 2022 года предпосылок, изменяющих отношение к риску технологической зависимости от поставщиков услуг. С массовым уходом зарубежных вендоров такие риски стали рассматриваться полноценно.

- Сложность получения объективных свидетельств о том, что уничтожение цифровых данных на стороне поставщика имело место.

- Зачастую незрелый процесс участия службы ИБ в процессе управления жизненным циклом ИТ-активов — приемка работ с точки зрения соответствия внутренним контролям и правилам ИБ не является системной практикой.

BAD PYRAMID



Распространенные проблемы данного этапа, чаще всего приводящие к инцидентам:

- Неполный контроль над инфраструктурой после прекращения взаимодействия
- Несвоевременная терминация учетных записей поставщиков
- Забытые тестовые и «временные» данные

Yellow Team

Наиболее ярко проблема неполного возврата полномочий характерна для технологического сегмента. Помимо программного «мусора» (средств удаленного управления, приложений 4G-модемов и пр.), подрядчики часто «забывают» передать реквизиты на системные или УЗ разработчиков.

В одном из кейсов администраторам ничего не оставалось, как «брутить» пароли на оборудование Cisco, к которому у них не оказалось доступа. Благо словарные пароли поддались довольно быстро.

Тестовые и «временные» данные мы обнаруживаем порой в самых необычных местах, например, в папках сервиса печати. Однажды мы обнаружили там резервные копии 1С с полным доступом к ним всех пользователей.

Red Team

Самые любимые места хранения «временных» скриптов для тестирования — общедоступные файловые директории, а также SYSVOL, NETLOGON, используемые для распространения объектов групповых политик и сценариев автоматизации.

На одном из проектов мы обнаружили в каталоге SYSVOL файл с конфигурацией VNC для доступа к системам управления производственной линией. Два клика могли остановить производственный процесс и привести к огромным финансовым потерям.

Стандартные пароли на служебные учетные записи MS SQL и другие сервисы, оставляемые подрядчиками после себя, также позволяют злоумышленнику получить доступ к конфиденциальной информации, а в случае ошибок конфигурации — к полной компрометации системы.

Blue Team

Особенно важно после завершения работы с подрядчиком проводить процесс инвентаризации внешнего периметра. Нередко после завершения работ подрядчики забывают убрать из публичного доступа «тестовую» инфраструктуру, на которой обкатывались разрабатываемые и внедряемые решения, либо подрядчик забывает закрыть публичный доступ к сервисам удаленного доступа. Наибольшей угрозой для Blue Team и ИТ-службы является то, что подобные «забытые куски» инфраструктуры находятся вне поля зрения, в связи с чем вовремя заметить угрозу становится сложно.

Один из последних кейсов: подрядчик принял решение в качестве удаленного доступа к тестовой инфраструктуре временно использовать протокол RDP, при этом не поставил в известность заказчика. После окончания работ протокол по-прежнему был публично доступен, а впоследствии стал точкой входа злоумышленников, подобравших пароль.

КАК СЕБЯ ОБЕЗОПАСИТЬ?

РЕКОМЕНДАЦИИ

Комплекс мер по управлению рисками эксплуатации доверия необходимо рассматривать в контексте **модели управления жизненным циклом взаимодействия**[5]. Модель представляет собой организационно-техническую систему, обеспечивающую управление рисками информационной безопасности на протяжении **всего процесса взаимодействия**, начиная с планирования взаимоотношений с поставщиком и заканчивая расторжением контракта.

Jet Security Trusted Relationship Framework (JSTRF), разработанный командой АО «Инфосистемы Джет», представляет собой набор контролей безопасности, уже структурированных с учетом модели жизненного цикла:

- Планирование взаимоотношений с поставщиком
- Оценка и выбор поставщиков
- Закрепление обязанностей сторон
- Инициализация взаимодействия
- Управление взаимоотношением
- Прекращение работы

JSTRF рассматривает специфичные риски информационной безопасности для каждого из этапов и может служить основой обеспечения эффективной информационной безопасности.

Для внедрения фреймворка рекомендуется выполнить следующие укрупненные шаги.

[5]«Жизненный цикл» поставщика - совокупность стадий развития отношений с поставщиком, которые проходит компания в процессе взаимодействия

1. **Проработать методическую базу и необходимую контрольную среду**

   Определить аспекты управления риском поставщиков услуг и заложить основы функционирования процесса.

   На этом этапе рекомендуется выбрать контроли безопасности, которые будут считаться минимальными и достаточными. Контроли являются гибко настраиваемым инструментом и должны выбираться с учетом специфики взаимодействия с поставщиками услуг и их критичности — профиля риска поставщика.

   Такие профили позволяют выбрать соответствующий базовый набор и быстро применять его для схожих типов поставщиков. JSTRF уже имеет в своем составе профили риска для типовых поставщиков, которые адаптируются под специфику компании:

   - Аудиторские компании
   - Провайдеры сервисных услуг
   - Внештатные работники
   - Другие

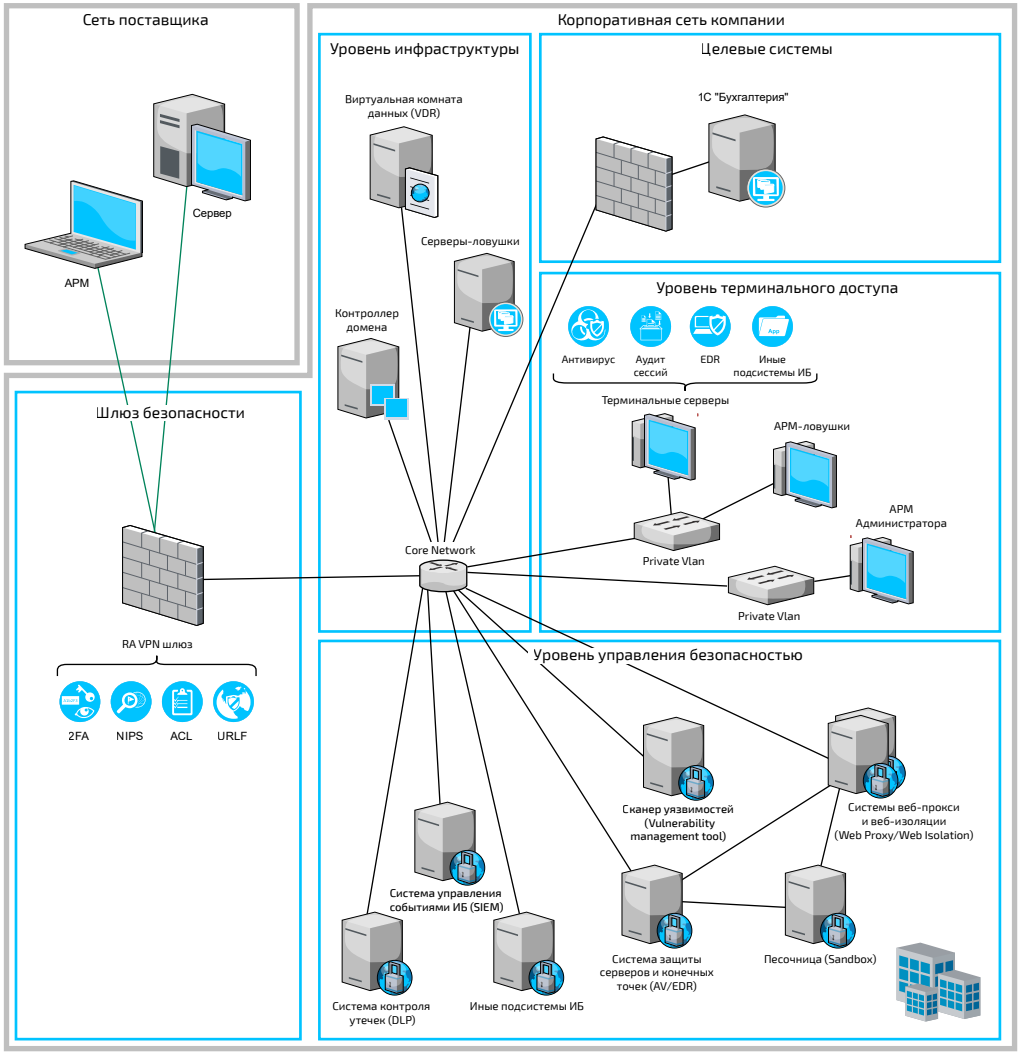
2. **Проработать методическую базу и необходимую контрольную среду**

   Обеспечить безопасную буферную зону и защиту сегмента инфраструктуры, предназначенного для совместного взаимодействия.

   Чтобы быстро и безопасно проводить онбординг новых поставщиков, рекомендуется унифицировать способы подключения поставщиков путем разработки **типовых архитектурных решений при взаимодействии** с использованием контролей JSTRF.

Такие решения представляют собой безопасную зону со средствами мониторинга и необходимыми средствами защиты. Создать ее можно как на терминальных серверах, так и на отдельных технических решениях, например, на системе класса PIM/PAM (Privileged Access/Identity Management).

Рекомендуется заранее подготовить такие типовые решения, при этом под разные задачи и возможности поставщиков их может быть несколько. Ниже приводится пример подобной типовой архитектуры.



Для выявления аномалий в поведении поставщиков и реакции на инциденты ИБ рекомендуется обеспечить мониторинг событий ИБ для совместно используемых ресурсов, построив профили поведения учетных записей подрядчиков.

Такой мониторинг не должен ограничиваться только внутренней инфраструктурой — рекомендуется включать в область анализа цифровые риски, возникающие за пределами корпоративного периметра:

- Мониторинг даркнета и Телеграм-каналов на предмет утечек (для выявления событий, свидетельствующих о взломе)
- Мониторинг поверхности атаки (для оценки защищенности внешнего периметра критичных поставщиков)

3. Интегрировать подход в существующие контракты

Пересмотреть существующие контракты (при продлении или поэтапно, начиная с критичных поставщиков) и применить меры безопасности для существующих поставщиков.

Повышение прозрачности уже существующих цепочек взаимодействия рекомендуется начать с шагов по инвентаризации услуг сторонних поставщиков и способов взаимодействия с последующим профилированием таких поставщиков.

О НАС

Центр информационной безопасности компании **«Инфосистемы Джет»** — профессиональное сообщество специалистов по ИБ. Мы защищаем коммерческие компании и государственные организации от киберугроз уже более 25 лет. Сегодня наша команда — это более 450 экспертов в области информационной безопасности, которые реализуют порядка 300 комплексных проектов в год для защиты бизнеса от киберугроз в России и СНГ.

НАША ГЛАВНАЯ ЗАДАЧА – СОЗДАНИЕ И ВНЕДРЕНИЕ СИСТЕМ, ОБЕСПЕЧИВАЮЩИХ РЕАЛЬНУЮ БЕЗОПАСНОСТЬ БИЗНЕСА.

О КОМПАНИИ

«Инфосистемы Джет» — одна из крупнейших ИТ-компаний в России. С 1991 года работает на рынке системной интеграции, реализуя ежегодно более 1000 проектов. Штат — более 2000 сотрудников.

Входит в ТОП-5 поставщиков ИТ-услуг России (IDC, 2021 г.). Лидер на рынке ИТ-аутсорсинга в России (Tadviser, 2022 г.). № 1 среди крупнейших поставщиков инфраструктуры дата-центров (Cnews, 2022 г.). № 2 среди крупнейших интеграторов в сфере защиты информации (CNews Analytics, 2022 г.), № 2 среди крупнейших поставщиков для промышленности (Tadviser, 2022 г.), № 2 среди крупнейших поставщиков для российских банков (Tadviser, 2022 г.).

Ключевые направления деятельности «Инфосистемы Джет»: ИТ-инфраструктура, сети и инженерные системы, ИТ-аутсорсинг, информационная безопасность, машинное обучение, заказная разработка ПО, внедрение и сопровождение бизнес-приложений Enterprise-уровня, промышленная безопасность и IoT.

В компании разработана собственная линейка продуктов, кроме того, «Инфосистемы Джет» располагает виртуальным ЦОД и крупнейшим на территории Восточной Европы сервисным центром. За 30 лет заказчиками компании стали более 1000 предприятий.