ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Network Traffic Analysis»

Описание процессов, обеспечивающих поддержание жизненного цикла

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Определение**
АС	Автоматизированная Система
Заказчик	Зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение.
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО БУДУЩЕЕ; • Компанией-интегратором, по выбору Заказчика
ЛВС	Локальная вычислительная сеть
ОС	Операционная Система
ПО	Программное обеспечение F6 Network Traffic Analysis, NTA.
ТС	(«Технический Сервис») Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Network Traffic Analysis». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
CEF	Common Event Format
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
JSON	JavaScript Object Notation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
Kerberos	Система аутентификации

LAN	Local Area Network
MDP	F6 Malware Detonation Platform
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
MXDR Console	F6 XDR, MXDR
NTLM	NT LAN Manager
RDP	Remote Desktop Protocol
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TI	Threat intelligence
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процессов поддержания жизненного цикла программного обеспечения «F6 Network Traffic Analysis» (далее – ПО, Network Traffic Analysis, NTA). Поддержание жизненного цикла ПО осуществляется за счет его сопровождения в течение всего периода эксплуатации и совершенствования (проведения обновлений) согласно собственному плану разработки и по заявкам Пользователей.

1.2 Назначение ПО

«F6 Network Traffic Analysis» — это программное обеспечение для обнаружения и реагирования на сетевые угрозы (Network Detection and Response), предназначенное для мониторинга, анализа и предотвращения кибератак в режиме реального времени. ПО предоставляет комплексный мониторинг сетевого трафика, анализируя его для выявления подозрительных действий и угроз. Используя передовые методы, такие как поведенческий анализ, машинное обучение и сигнатурный анализ, ПО может обнаруживать сложные атаки, в том числе сетевые атаки, использование вредоносного ПО, фишинговые атаки и эксплуатацию уязвимостей. Благодаря интеграции с другими продуктами АО «БУДУЩЕЕ», такими как «F6 Threat Intelligence», ПО повышает точность обнаружения угроз и позволяет более эффективно управлять инцидентами безопасности.

ПО также поддерживает функции охоты на угрозы (Threat Hunting) и проведения форензики, что позволяет специалистам детально анализировать инциденты и выявлять их причины и последствия.

Выявление вредоносной активности, аномалий и скрытых каналов в сетевом трафике осуществляется в несколько шагов:

1. Сетевой трафик проходит через модуль сигнатурного анализа.
2. Трафик сети анализируется с помощью ML-классификаторов.
3. Сетевые сигналы (алерты) автоматически соотносятся с другими инцидентами в XDR для последующего анализа.
4. Выделенные из потока объекты отправляются на анализ в MDP платформу контролируемого запуска («детонации») вредоносных программ.

5. В XDR отправляются подробные сетевые логи для проактивного поиска недетектируемых угроз.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

– ПО реализуется в виде программно-аппаратного комплекса для установки в стандартную 19-дюймовую стойку с наличием как минимум одного интерфейса 1000BASE-T для захвата сетевого трафика и одного интерфейса 1000BASE-T для управления и подключения к ЛВС.

– Подключение осуществляется к интерфейсу копии сетевого трафика без влияния на работу ЛВС и без вмешательства в анализируемое сетевое взаимодействие.

– По осуществляет захват сетевых фреймов на уровне L2, восстановление пакетов L4 - L7 и реализует следующие функций:

  – Сигнатурный анализ трафика на основе базы решающих правил.

  – Выявление инкапсуляции данных в трафике, включая ICMP tunneling, DNS tunneling, HTTP tunneling, DGA.

  – Запись трафика и сохранение его на сетевом хранилище в формате .pcap.

  – Регистрация информации обо всех сетевых соединениях на уровне TCP, UDP, IP, ICMP с фиксацией времени, числа пакетов и объема переданных данных.

  – Регистрация информации о DNS-запросах с фиксацией времени, источника и получателя запроса, содержимого запроса и ответа.

  – Регистрация информации о HTTP-запросах с фиксацией времени, источника и получателя, метода, URI и всех заголовков.

  – Регистрация информации о соединениях по протоколам RDP, SMB, DHCP, FTP, Kerberos, NTLM, SMTP, SSH, Telnet, SSL.

– ПО выявляет попытки горизонтального перемещения, атакующего внутри ЛВС и передает соответствующую информацию в XDR для формирования события информационной безопасности.

– ПО поддерживает обработку каналов с консолидированной пиковой загрузкой до 1 Гбит/сек.

– ПО имеет озможность инвентаризации сетевого оборудования и конечных устройств в пассивном режиме.

- ПО осуществляет передачу в XDR параметры телеметрии для отслеживания аварийных ситуаций, перегрузок и параметров работы, включая:
  - Количество выделенной и свободной памяти.
  - Среднюю загрузку процессора по ядрам.
  - Число пакетов, поступивших на интерфейсы приема трафика.
  - Общий объем данных, поступивших на интерфейсы приема трафика.
  - Объем свободного пространства на жестком диске.
- Передача телеметрии и информации о событиях осуществляется через механизм Syslog в форматах JSON и CEF для интеграции с другими системами.

2 Процесс разработки ПО

Процесс разработки ПО включает в себя:

- Сбор и анализ требований к разработке ПО;
- Проектирование архитектуры ПО;
- Разработка ПО в коде;
- Проведение тестирования ПО перед эксплуатацией;
- Запуск в промышленную эксплуатацию ПО;
- Промышленная эксплуатация ПО;
- Сопровождение ПО.

2.1 Сбор и анализ требований к разработке ПО

На этапе сбора и анализа требований ПО определяются требования всех заинтересованных сторон, включая функциональные и нефункциональные требования.

Основные этапы сбора и анализа требований к разработке ПО:

- Определение основных задач и целей, которые должен решить проект ПО;
- Определение ключевых заинтересованных сторон (заказчики, пользователи, разработчики, другой персонал);
- Сбор требований к ПО;
- Анализ требований, их уточнение, пересмотр на точность и реализуемость;
- Оценка рисков;
- Создание плана и графика реализации проекта;
- Документирование требований и проектных планов;
- Согласование и утверждение требований.

2.2 Проектирование архитектуры ПО

Проектирование архитектуры ПО – это процесс определения общей структуры системы, ее компонентов и модулей, а также взаимодействия между компонентами системы на основе выработанных требований.

Проектирование архитектуры включает в себя следующие этапы:

– Определение архитектурного стиля;

– Определение основных модулей и компонентов системы, их взаимодействие;

– Выбор технологий (языки программирования, базы данных и т.д.) и инструментов для разработки ПО;

– Документирование архитектуры системы.

2.3 Разработка ПО в коде

На этапе разработки ПО в коде осуществляется реализация проектных решений с помощью выбранных технологий и инструментов.

Разработка ПО включает в себя следующие этапы:

– Написание исходного кода ПО с использованием выбранных технологий и инструментов;

– Проверка кода на наличие ошибок и несоответствий;

– Проведение интеграционного тестирования;

– Отладка кода (исправление обнаруженных ошибок);

– Проверка кода для улучшения качества ПО, его производительности и безопасности;

– Интеграция частей кода и модулей ПО в единую систему, проверка их совместимости;

– Подготовка к тестированию ПО перед эксплуатацией.

2.4 Проведение тестирования ПО перед эксплуатацией

Тестирование ПО перед эксплуатацией – это оценка качества ПО, его функциональности, производительности и безопасности. Цель тестирования заключается в подтверждении того, что ПО удовлетворяет установленным требованиям и корректно работает в различных условиях. Тестирование включает в себя следующие этапы:

– Автоматические unit-тесты, встроенные в pipeline CI/CD процессов при работе с репозиторием хранения исходного кода;

– Автотесты с использованием Allure (pytest + selenium) с покрытием не менее 35%;

– Полуавтоматическое регрессионное тестирование на каждую вновь добавляемую новую функцию;

– Ручное тестирование: интеграционное, функции, API.

После ручного тестирования и добавления каждой функции в ПО, ручное тестирование автоматизируется и добавляется в общий банк автотестов.

2.5 Запуск ПО в промышленную эксплуатацию

Запуск в промышленную эксплуатацию – это процесс подготовки окружения для развертывания ПО на целевой среде Заказчика, а также установка и активация модуля. Запуск в промышленную эксплуатацию осуществляется силами Исполнителя.

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности XDR.

ПО разворачивается в сетевой инфраструктуре заказчика.

2.5.1 Проверка физической работоспособности NTA

1. Проверить наличие и размещение оборудования Системы.
2. Проверить подачу питания на серверы Системы.
3. Проверить интеграцию с инфраструктурой заказчика.
4. Убедиться, что оборудование включается при нажатии кнопки включения.

2.5.2 Проверка корректности загрузки исполняемого программного обеспечения NTA

1. После корректной загрузки программного обеспечения на устройствах Системы отображается поле для ввода логина и пароля на вход в программную оболочку.
2. После входа в программную оболочку проверить статус соединения с MXDR Console: Huntbox connection - OK.

2.5.3 Проверка связности модулей XDR с Malware Detonation Platform

После загрузки ПО необходимо проверить инфраструктурную связь модуля с другими компонентами системы.

1. Проверить наличие доступов, прописанных в карте взаимодействия.
2. При наличии локальной MXDR Console: перейти в раздел **Настройки** → **Модули** → **MXDR Console** → **Основные настройки** и добавить запись MDP из выпадающего списка доступных MDP модулей. Проверить, что статус модуля в настройке интеграции зеленый.

3. При наличии модуля NTA: перейти в раздел **Настройки** → **Модули** → **Network Traffic Analysis** → **Основные настройки** → **Интеграция с MDP** и добавить запись MDP (локальная или облачная). Проверить, что статус модуля в настройке интеграции зеленый.

2.5.4 Проверка поступления зеркалированного трафика на сетевые интерфейсы NTA и корректности обработки этого трафика

1. Проверить наличие прописанных сетей для анализа/исключений:

Перейти в раздел **Настройки** → **Модули** → **Network Traffic Analysis** → **Общие настройки** → **Сетевой трафик** → **Анализ сетевого трафика** и проверить наличие указанных домашних подсетей, подлежащих анализу, а также подсетей/адресов, исключаемых из анализа (Через настройки Белого списка или BPF фильтр).

2. Проверить активность модуля сигнатурного анализа:

– в программной оболочке NTA Engine status в состоянии OK;

– в разделе **Настройки** → **Модули** → **Network Traffic Analysis** → **Общие настройки** → **Сетевой трафик** → **Сетевые сигнатуры** → **Статус** “ON”. (Можно оставить включенные по умолчанию пакеты сигнатур).

3. Проверить корректность интеграции модуля и подачи трафика:

Индикатор состояния устройства в разделе **Настройки** → **Модули** → **Network Traffic Analysis** зеленый, а график **span** трафика/значение загрузки канала соответствуют ожидаемому значению (например, уровню среднего уровня загрузки канала сети организации).

4. Провести тестирование качества поданного трафика и наличие детекта:

o С устройства внутри инфраструктуры, трафик которого зеркалируется на NTA, перейдите по ссылке: https://trebuchet.f6.security/?tab=network (Нет необходимости использовать тестовую машину, так как в проводимом далее тестировании отсутствует реальная вредоносная нагрузка).

o В окне введите "start" и нажмите клавишу Enter.

o В Web-интерфейсе XDR проверьте наличие тестовых событий в разделе **Атаки** → **Алерты**.

o IP-адрес узла, с которого был проведен тест, должен отражаться в теле алерта.

– Детектирование синтетических запросов, генерируемых в процессе теста, указывает на следующее:

o Трафик тестового стенда действительно зеркалируется на NTA.

- NTA получает пригодные для сборки сессий кадры.
- NTA готов осуществлять детектирование угроз в сети предприятия.

2.5.5 Проверка функциональности сбора метаинформации о сетевых соединениях

1. Проверить, что зеркалированный трафик корректно поступает на сетевые интерфейсы NTA (см. предыдущий пункт), а график span трафика/значение загрузки канала соответствуют ожидаемому значению (например, среднему уровню загрузки канала сети организации).

2. Проверить наличие настройки сбора метаинформации устройством:

3. Перейти в раздел **Настройки → Модули → Network Traffic Analysis → Общие настройки → Сетевой трафик → Сбор метаинформации о сетевых соединениях** и перевести в статус ON сбор метаинформации по конкретным или всем перечисленным в разделе протоколам.

4. Перейти в раздел **Расследование → Сетевые соединения** и проверить наличие данных в разделе (заложить время ~ 5 мин.).

2.5.6 Подсистема интеграции по протоколу ICAP

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности XDR и MDP, а также наличие корректной интеграции NTA с MDP.

1. Настройка инфраструктуры на стороне Заказчика:

Поддержка работы по протоколу ICAP в режиме respmod, сетевая доступность между прокси и NTA, настройка отправки данных на указанный адрес (IP-адрес модуля NTA) и назначенный порт.

2. Настройка ICAP на NTA:

Перейти **Настройки → Модули → Название Модуля → Общие настройки → Сетевой трафик → ICAP-сервер** “ON” (при необходимости сменить порт, если прокси передает файлы по другому порту) → **Блокировать скачиваемые вредоносные файлы** “ON”

3. Выбрать тестовый компьютер и перейти на http://threattest.group-ib.tech/icap/ (именно HTTP) и скачать файл на тестовый компьютер.

4. Проверить получение информации о загрузке файла в разделе **Расследование → Проверенные файлы (Фильтр → Источник файла “ICAP”)** и наличие вердикта по файлу (вредоносный).

5. Проверить функциональность блокировки загрузки файла в разделе **Атаки** → **Алерты**, система интеграции ICAP-сервер (выбрать в фильтрах справа).

6. В случае, если алерт и информация о файле отсутствуют, необходимо провести повторный анализ совместно с инженерами АО «БУДУЩЕЕ».

2.5.7 Подсистема интеграции с общими ресурсами

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности MXDR Console и MDP, а также наличие корректной интеграции NTA с MDP.

1. Настройка инфраструктуры на стороне заказчика: сетевая доступность между NTA и файловым хранилищем, наличие отдельной учетной записи для доступа в хранилище, поддержка работы по протоколам.

2. Настройка интеграции на NTA:

Перейти в раздел **Настройки** → **Модули** → **Network Traffic Analysis** → **Основные настройки** → **Общие настройки** → **Монтирование общих ресурсов**, добавить новый ресурс. Для добавления необходимо добавить адрес хранилища, выбрать протокол доступа и ввести учетные данные для доступа. После добавления ресурса должны появиться данные о загрузке хранилища и индикатор успешного статуса интеграции.

3. Настройка режима работы с файловым хранилищем и анализа файлов:

Перейти в раздел **Настройки** → **Модули** → **NTA** → **Основные настройки** → **Файлы** → **Анализ общих ресурсов** и добавить запись о режиме работы для любого из доступных для настройки хранилищ.

4. Проверить работоспособность интеграции:

Перейти в раздел **Расследование** → **Проверенные файлы**, установить фильтр **Источник файла** в значение **DIR**.

5. Наличие файлов в данном режиме фильтрации свидетельствует о корректной интеграции с файловым хранилищем.

2.5.8 Модуль извлечения файлов из трафика

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности MXDR Console и MDP, а также наличие корректной интеграции NTA с MDP.

1. Проверить, что зеркалированный трафик корректно поступает на сетевые интерфейсы NTA: Настройки → **Модули** → **Network Traffic Analysis** → **Индикатор** слева горит зеленым, а график span трафика/значение загрузки канала соответствуют ожидаемому значению (например, уровню среднего уровня загрузки канала сети организации).

2. Если MDP установлен локально, то необходимо убедиться, что на MDP нет очереди:

Перейти в раздел **Настройки** → **Модули** → **Malware Detonation Platform** → **На графике состояния** модуля во вкладке **Задачи** нет очереди.

3. Проверить, что включена опция извлечения файлов и протоколы для извлечения: **Настройки** → **Модули** → **Название Модуля** → **Общие настройки** → **Файлы** → **Анализ файлов из трафика** → **Протоколы** → **“Название протокола” – ON**.

4. Провести загрузку файла по протоколу HTTP (Ссылка на файл будет предоставлена вендором).

5. Проверить результаты тестирования в разделе **Расследование** → **Проверенные файлы**, установив фильтр **Источник файла** в значение протоколов, по которым происходит извлечение (HTTP).

2.6 Промышленная эксплуатация

Промышленная эксплуатация (далее – Эксплуатация) – это этап жизненного цикла, когда установленное ПО используется в реальных рабочих условиях на постоянной основе.

Эксплуатация включает в себя следующие этапы:

- Аналитическое сопровождение и работы по выявлению аномалий и мошеннической активности среди клиентов Заказчика;
- Обработка выявляемых событий и предоставление обратной связи;
- Тонкая настройка правил выявления мошеннической активности;
- Контроль работоспособности АС Заказчика;
- Контроль работоспособности ПО;
- Доработка и регулярное обновление ПО для устранения ошибок, повышения производительности, а также введения новых функций;
- Периодическая отчетность по работоспособности и устранениям неисправностей ПО;

– Поддержка актуальной документации.

2.7 Сопровождение ПО

В течение всего периода эксплуатации ПО Заказчику предоставляется сопровождение ПО, в рамках которого оказываются следующие услуги:

– Техническая поддержка Пользователей;

– Решение инцидентов (экстренных неисправностей), возникающих в процессе эксплуатации ПО;

– Устранение сбоев и ошибок, выявленных в ПО;

– Совершенствование ПО;

– Мониторинг производительности ПО;

– Оптимизация эффективности работы ПО;

– Поддержка актуальной технической документации по ПО;

– Уведомление об обновлениях и изменениях ПО;

– Обучение новых пользователей.

3 Совершенствование ПО

ПО на постоянной основе подвергается развитию и улучшению в рамках процессов:

– развития и добавления новых функциональных возможностей, позволяющих расширить области применения ПО;

– оптимизации работы модулей ПО, обеспечивающей повышение производительности, скорости обработки данных и отказоустойчивости;

– обновления пользовательского интерфейса.

Совершенствование ПО происходит за счет проведения модернизаций ПО в соответствии с собственным планом доработок, а также с учетом заявок клиентов по вопросам испытаний установки и эксплуатации, полученных через ТС.

4 Устранение неисправностей ПО

Неисправности, которые были выявлены в ходе полноценной эксплуатации ПО, могут быть исправлены следующими способами:

- Массовое обновление компонентов ПО;
- Единичная работа технического специалиста по запросу Пользователя.

В случае возникновения неисправности клиент направляет заявку через Технический Сервис (далее – ТС) Разработчика с подробным описанием воспроизведенной проблемы (версия ПО, описание конфигурации, версия приложения клиента, прикрепленные скриншоты). Затем технический специалист проводит следующие действия:

- подтверждает наличие неисправности в соответствии с описанием проблемы от Заказчика;
- тестирует неисправность в функционале ПО и создает отчет по результатам тестирования;
- фиксирует задачу на исправление проблемы в текущий или ближайший релиз обновления ПО или консультирует клиента по корректности выполняемых действий.

Задачи по устранению неисправностей в функционале ПО осуществляются силами Разработчика. В соответствии с внутренним планом выхода обновлений подсистемы предоставляется исправленный механизм работы ПО.

Процессы по устранению неисправностей протекают непрерывно, без остановки функционирования ПО.

4.1 Устранение экстренных неисправностей ПО

В экстренном случае, когда ошибка препятствует полноценному использованию функционала ПО, группа разработчиков готовит внеплановый выход обновления или предоставляет исправленную версию ПО.

При возникновении экстренных неисправностей Заказчик отправляет запрос через ТС со следующими данными:

- Четко сформулированная тема обращения;
- Версия приложения заказчика, на которой осуществляется эксплуатация ПО;
- Версия ПО;

- Пошаговое описание воспроизведения ошибки;
- Скриншоты, демонстрирующие наличие найденной ошибки.

5 Техническая поддержка

Техническая поддержка Пользователей осуществляется в соответствии с условиями контракта следующими способами:

- Приоритетный способ осуществления техподдержки через создание запросов во вкладке «Поддержка» по ссылке https://xdr.f6.security/service-desk
- по электронной почте: info@f6.ru;
- по номеру телефона: +7 495 984-33-64;

В рамках технической поддержки оказываются следующие услуги:

- консультация по фактическому наличию имеющегося функционала в системе;
- помощь в настройке и интеграции ПО;
- помощь в эксплуатации ПО;
- решение технических проблем;
- пояснение принципов работы имеющихся механизмов ПО;
- поиск, тестирование и фиксирование найденных ошибок;
- предоставление актуальной документации по настройке, эксплуатации и работе ПО.

Время работы технической поддержки: с понедельника по пятницу с 9:00 до 18:00 UTC+3.

Фактический адрес размещения службы поддержки ПО «F6 Network Traffic Analysis»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

6 Информация о персонале

6.1 Персонал, обеспечивающий работу ПО на рабочих местах пользователей

К эксплуатации ПО допускаются лица, ознакомившиеся с документацией по эксплуатации ПО в разделе «Помощь» пользовательского интерфейса ПО.

К эксплуатации ПО привлекается штатный персонал Заказчика, имеющий следующие навыки:

- навыки работы с персональным компьютером на уровне опытного пользователя;
- опыт работы с электронными документами;
- опыт использования web-браузеров;
- Знания в соответствующей предметной области.

6.2 Персонал, обеспечивающий техническую поддержку, аналитическую поддержку и модернизацию ПО

Специалисты, обеспечивающие техническую и аналитическую поддержку и развитие ПО, должны обладать следующими знаниями и навыками:

- знание функциональных возможностей ПО;
- знание особенностей работы с ПО;
- знание языков программирования, исходя из должностных обязанностей: Python, GO, Rust, JavaScript, TypeScript;
- знание реляционных и не реляционных БД, исходя из должностных обязанностей: PostgreSQL, Elasticserch, ClickHouse, MongoDB;
- знание средств мониторинга производительности серверов.

– Должность	**Компетенции**	**Выполняемые работы**	**Количество специалистов**
Backend разработчик	Go, Python, Zeek, Zuricata	Техническая поддержка; Аналитическое сопровождение; Разработка и совершенствование ПО.	3

DevOps инженер	Linux, Ansible, Docker, GitLab CI\CD, Elasticsearch, PostgreSQL, Minio.	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2
Анатилик разработки детектирующей логики	Python, Zeek, Suricata	Техническая поддержка; Аналитическое сопровождение; Совершенствование ПО.	2
Тестировщики	Allure, Pytest, Gitlab CI/CD, Разработка авто тестов, функционального и нагрузочного тестирования	Разработка тест-планов для тестирований продуктового функционала; Проведение ручного тестирования согласно разработанным планам; Разработка автоматических тестов и анализ его результатов; Проведение регрессионного тестирования.	2

ИНФОРМАЦИЯ О ФАКТИЧЕСКИХ АДРЕСАХ

Фактический адрес размещения разработчиков ПО 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

Фактический адрес размещения службы поддержки ПО 115088, г. Москва, ул. Шарикоподшипниковская, д. 1

Контакты службы поддержки:

- Электронная почта: info@f6.ru
- Телефон: +7 495 984-33-64

Информация о фактическом адресе размещения инфраструктуры разработки ПО

ПО может поставляться в виде облачного сервиса, в таком случае ПО размещается на удаленных серверах компании АО «Селектел» по адресу:

188683, Ленинградская область, Всеволожский район, г.п. Дубровка, ул. Советская, дом 1, литера Б.