F6

Акционерное общество «Будущее»
ОГРН: 1247700295721
ИНН/КПП: 9709109340/772301001

115088, г. Москва,
ул. Шарикоподшипниковская, д. 1,
помещ. 14/9

Специальные условия оказания услуг «SOC MDR F6»

Версия 1.0. от 25.12.2025 г.

F6

История изменений

Версия	Изменения	Дата публикации
1.0	Введение в действие	25.12.2025

F6

Оглавление

1 СОКРАЩЕНИЯ

- **ИБ** – информационная безопасность.
- **ПО** – программное обеспечение;
- **F6** – лицо, оказывающее услуги Заказчику (непосредственный исполнитель), а именно акционерное общество «Будущее» (ИНН 9709109340, ОГРН 1247700295721, адрес местонахождения: 115088, г. Москва, вн. тер. г. Муниципальный округ Южнопортовый, ул. Шарикоподшипниковская, д. 1, помещ. 14/9);
- **SLA** (Service Level Agreement) — соглашение об уровне обслуживания между Заказчиком и F6.

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- **F6 XDR** – программное обеспечение «F6 Extended Detection and Response», функциональностью которого является комплексное выявление признаков кибератак путем анализа, корреляции данных, принятия решений с целью управления рисками информационной безопасности ИТ-инфраструктуры.
- **F6 EDR** – программное обеспечение «F6 Endpoint Detection and Response», предоставляемое отдельно или в составе F6 XDR, функциональностью которого является фиксация и блокировка аномального поведения, изоляция устройства, отправка данных в удаленное хранилище для последующего анализа.
- **Агент F6 EDR** – компонент **F6 EDR**, устанавливаемый на конечные устройства.
- **F6 NTA** – программное обеспечение «F6 Network Traffic Analysis», предоставляемое в составе F6 XDR, функциональностью которого является отслеживание подозрительной активности в компьютерной сети.

- **F6 ASM** – программное обеспечение «F6 Attack Surface Management», функциональностью которого является оценка поверхности атаки и управление ею через облачный пользовательский интерфейс.
- **RACI-матрица** – таблица, с помощью которой распределены полномочия и роли Заказчика и F6 в рамках Услуги.
- **SIEM** – система сбора и корреляции событий безопасности для контекстного анализа инцидентов.
- **Веб-портал** — интерфейсная часть программного обеспечения F6, доступ к которой осуществляется через веб-браузер после прохождения процедур аутентификации и авторизации.
- **Актив** – любой компонент информационной инфраструктуры Заказчика, имеющий ценность и подлежащий защите в рамках оказания Услуг.
- **Событие ИБ** – любое идентифицированное изменение состояния или активности в системе, сети или активах Заказчика, которое может иметь значение для информационной безопасности Заказчика.
- **Угроза (ИБ)** – совокупность условий и факторов, направленных на компрометацию активов Заказчика. Следствием этой компрометации является или может являться нарушение конфиденциальности, целостности, доступности информации или причинение иного ущерба.
- **Алерт** – автоматически сгенерированное системой мониторинга или защиты уведомление о возникновении события ИБ, которое по заданным критериям указывает на возможную угрозу и требует верификации.
- **Проблема** – выявленная с использованием F6 ASM проблема безопасности, которая по заданным критериям указывает на возможную угрозу и требует верификации.
- **Верификация** – выполняемый F6 процесс анализа алерта или проблемы для подтверждения факта реализации угрозы или вероятности возможность реализации. По результатам верификации определяется наличие или отсутствие инцидента.
- **Инцидент** – подтвержденный в процессе верификации факт успешной реализации или попытка реализации угрозы, которая привела или может привести к нарушению политик безопасности, несанкционированной деятельности, оказавшей или способной оказать негативное влияние на активы Заказчика.
- **Реагирование (на инцидент)** – комплекс действий F6, инициируемых после подтверждения инцидента и направленных на минимизацию его последствий. В зависимости от состава Услуг действия могут включать в себя уведомление Заказчика

с предоставлением рекомендаций по нейтрализации угрозы или активные действия по самостоятельной нейтрализации угрозы силами F6.

- **Услуги** – комплексная услуга «SOC MDR F6», включающая в себя следующие услуги, оказываемые в совокупности или по отдельности:
  - круглосуточный мониторинг и выявление инцидентов ИБ[1];
  - оперативное реагирование на инциденты ИБ;
  - проактивный поиск недетектируемых угроз.

[1] *Альтернативное наименование*: Комплексный круглосуточный мониторинг и выявление инцидентов ИБ.

3 РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ И SLA

3.1. УСЛУГА: Круглосуточный мониторинг и выявление инцидентов ИБ

3.1.1. НАИМЕНОВАНИЕ УСЛУГИ:
Круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО F6 ASM

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования F6 ASM.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного мониторинга и анализа внешней инфраструктуры Заказчика для своевременного выявления инцидентов и предотвращения реализации угроз.

1.4. В рамках оказания Услуги F6 осуществляет:

- выявление проблем ИБ на внешних цифровых активах, относящихся к инфраструктуре Заказчика;
- автоматическую классификацию выявленных проблем по уровню критичности (опасности);
- верификацию и анализ проблем, исследование на предмет компрометации;
- информирование Заказчика о подтвержденных проблемах;
- предоставление рекомендаций по устранению проблем;
- предоставление отчета.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются только для внешних активов, подтвержденных Заказчиком в Веб-портале F6 ASM.

2.2. Устранение выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по устранению проблем в рамках данной Услуги.

2.3. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который был реализован:

- на активе, не включенном в область применения Услуги;
- на активе, который был помечен в Веб-портале F6 ASM Заказчиком как «лишний или игнорируемый»;
- через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных является F6 ASM, которое обеспечивает:

- автоматизированное сканирование внешнего сетевого периметра Заказчика;
- анализ и корреляцию данных для определения критичности (опасности) выявленных проблем.

3.3. Сканирование выполняется без вмешательства в инфраструктуру Заказчика и предназначено для выявления потенциальных уязвимостей, небезопасных конфигураций, а также индикаторов подозрительной или вредоносной активности.

3.4. Политика ответственного сканирования, а также информация о методах и объектах сканирования представлены на сайте https://scan.f6.security/.

3.5. На основе анализа собранных данных автоматически формируются проблемы, которые:

- отображаются в Веб-портале F6 ASM в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Сформированным проблемам автоматически присваивается статус:

Статус	Описание
Обнаруженные	Все обнаруженные проблемы
Решенные	F6 ASM не обнаружило наличие проблемы при повторной проверке

4.2. Сформированным проблемам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Критичная опасность	Требует немедленного вмешательства
Высокая опасность	Требует скорейшего вмешательства
Средняя опасность	Требует повышенного внимания
Низкая опасность	Потенциально незначительный ущерб

4.3. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. Анализ проблем со стороны F6 производится только в отношении **подтвержденных** активов Заказчика.

5.2. Заказчик осуществляет классификацию выявленных активов в Веб-портале F6 ASM, используя статусы:

- «**подтвердить**» – актив принадлежит инфраструктуре Заказчика;
- «**лишние или игнорируемые**» – актив не относится к инфраструктуре Заказчика.

5.3. F6 анализирует подтвержденные проблемы **«Критичного»** и **«Высокого»** уровня по категориям:

- уязвимости;
- сетевая безопасность;
- утечки данных;
- вредоносные программы;
- упоминания в дарквебе.

5.4. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем.

5.5. Для верификации проблем могут привлекаться дополнительные программные инструменты F6.

5.6. По результатам верификации F6 устанавливает статус проблемы:

Статус	Описание
Ложно-позитивные	Проблема найдена ошибочно и не подтверждена F6
В работе	Проблема подтверждена, принята в работу F6

6. УВЕДОМЛЕНИЕ

6.1. Уведомление происходит при подтверждении проблемы.

6.2. F6 направляет Заказчику уведомление с указанием:

- краткого описания проблемы;
- списка затронутых активов;
- базовых рекомендаций по устранению проблемы.

6.3. В процессе исследования проблемы F6 может дополнять уведомление сведениями, включая:

- информацию о ходе и результатах исследования;
- дополнительные рекомендации по устранению проблемы.

6.4. Порядок направления уведомления — через Веб-портал F6 ASM, по электронной почте или иным способом, согласованным Сторонами.

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается проблеме, выявленной с использованием F6 ASM:

Условие	Критерий
Автоматически	При повторном автоматическом сканировании проблема отсутствует
Вручную F6	От Заказчика получена обратная связь об успешном выполнении рекомендаций F6 в полном объеме

7.2. Изменение статусов проблем фиксируется в Веб-портале F6 ASM и отражается в отчете.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца, включает:

- количество, категории и критичность выявленных проблем;
- перечень активов, на которых обнаружены проблемы;
- принятые меры и оставшиеся риски.

8.2. Оперативный отчет предоставляется по запросу Заказчика, включает:

- способ обнаружения проблемы;
- список затронутых активов;
- базовые рекомендации по устранению проблемы;
- рекомендации по локализации инцидента, в случае реализации угрозы посредством проблемы;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Сканирование активов и обнаружение проблем	+	-
Подтверждение активов в F6 ASM	-	+
Верификация проблем	+	-
Оповещение	+	-
Устранение проблем	-	+

10. SLA

Параметр	Условие	Срок
Верификация проблемы	Проблема критического или высокого уровня	До 4 часов
Оповещение Заказчика с предоставлением рекомендаций	Проблема критического или высокого уровня	До 1 часа с момента верификации обнаруженной Проблемы
Отчет	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.1.2. НАИМЕНОВАНИЕ УСЛУГИ:
Круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО F6 NTA

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования ПО:

- F6 NTA

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного:

- выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги F6 осуществляет:

- круглосуточный сбор, корреляция и анализ событий ИБ с сетевой инфраструктуры Заказчика;
- автоматическая классификация выявленных проблем и событий по уровню критичности (опасности);
- верификация выявленных проблем и событий ИБ, исследование на предмет компрометации, оформление инцидентов;
- информирование Заказчика об Инцидентах;
- формирование рекомендаций по реагированию со стороны Заказчика;
- подготовка отчетов.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются **только** для активов:

- находящихся в сетевых сегментах, трафик с которых поступает в F6 NTA;

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. Исправление выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по исправлению проблем в рамках данной Услуги.

2.4. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных является:

3.2.1. F6 NTA, с использованием которого осуществляется:

- анализ сетевого трафика;
- выявление аномалий, вредоносной активности, скрытых каналов связи и попыток эксплуатации уязвимостей.

3.3. На основе анализа собранных данных автоматически формируются проблемы и алерты, которые:

- отображаются в соответствующих Веб-порталах в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Алертам, сформированным с использованием F6 NTA, автоматически присваивается статус:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

Обнаруженным алертам автоматически присваивается уровень опасности:

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.2. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. Для F6 NTA:

5.1.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.1.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

5.1.3. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание

Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события ИБ отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза неприменима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

5.1.4. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем и алертов.

5.1.5. Для верификации проблем и алертов могут привлекаться дополнительные программные инструменты F6.

6. УВЕДОМЛЕНИЕ

6.1. При оформлении инцидента, сформированного на основе алерта в F6 NTA, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности;
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.2. В процессе расследования F6 дополняет сведения о проблеме или инциденте, включая:

- информацию о ходе и результатах анализа проблемы или инцидента;
- дополнительные рекомендации по реагированию на проблему или инцидент.

6.3. Порядок информирования:

Веб-портал	Условие	Способ коммуникации
F6 NTA	Высокая опасность	Через Веб-портал F6 XDR, по электронной почте и по телефону или иным способом, согласованным Сторонами
	Средняя опасность	Через Веб-портал F6 XDR или иным способом, согласованным Сторонами

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается инциденту в F6 NTA при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.2. Изменение статусов проблем и инцидентов фиксируется в соответствующих Веб-порталах и отражается в отчетах.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца:

8.1.1. Ежемесячный отчет об инцидентах, выявленных с использованием F6 NTA, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика:

8.2.1. Оперативный отчет об инциденте, выявленном с использованием F6 NTA, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;

- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Настройка F6 NTA	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10.SLA

Целевые показатели, применимые для использования F6 NTA:

F6

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчетность	Отчет об инциденте	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.1.3. НАИМЕНОВАНИЕ УСЛУГИ:
Круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО F6 EDR

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования F6 EDR.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги F6 осуществляет:

- круглосуточный сбор, корреляцию и анализ событий с конечных устройств в инфраструктуре Заказчика;
- автоматическую классификацию выявленных событий по уровню критичности;
- верификацию выявленных событий ИБ, оформление инцидентов;
- информирование Заказчика об инцидентах;
- расследование инцидентов;
- формирование рекомендаций по реагированию на инциденты;
- предоставление отчета.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются только для активов Заказчика, на которых установлены и функционируют агенты F6 EDR.

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе Заказчика, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6.

2.4. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных являются агенты F6 EDR, установленные на конечные устройства Заказчика, который проводит:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

3.3. На основе анализа собранных данных автоматически формируются алерты, которые:

- отображаются в Веб-портале в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Обнаруженным алертам автоматически присваиваются следующие статусы:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

4.2. Обнаруженным алертам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.3. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

5.3. F6 вправе запросить у Заказчика дополнительную информацию для верификации алертов.

5.4. Для верификации алертов могут привлекаться дополнительные программные инструменты F6.

5.5. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза не применима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

6. УВЕДОМЛЕНИЕ

6.1. При оформлении инцидента F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности.
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.2. В процессе расследования инцидента F6 может дополнять уведомление сведениями, включая:

- информацию о ходе и результатах анализа инцидента;
- дополнительные рекомендации по реагированию на инцидент.

6.3. Порядок направления уведомления:

- для инцидентов среднего уровня — через Веб-портал.
- для инцидентов высокого уровня — через Веб-портал и по телефону или иным способом, согласованным Сторонами.

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается инциденту в F6 EDR при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.2. Изменение статусов инцидентов фиксируется в Веб-портале и отражается в отчете.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Установка агентов F6 EDR	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10. SLA

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчеты	Оперативный отчет	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.1.4. НАИМЕНОВАНИЕ УСЛУГИ:
Круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО F6 XDR

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования F6 XDR.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги осуществляется:

- круглосуточный сбор, корреляция и анализ событий с конечных устройств и сетевой инфраструктуры Заказчика;
- автоматическая классификация выявленных событий по уровню критичности (опасности);
- верификация выявленных событий, оформление инцидентов;
- информирование Заказчика об инцидентах;
- расследование инцидентов;
- формирование рекомендаций по реагированию на инциденты;
- предоставление отчета.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются **только** для активов:

- на которых установлены и функционируют агенты F6 EDR, обеспечивающее сбор и передачу телеметрических данных;
- находящихся в сетевых сегментах, трафик с которых поступает в F6 NTA.

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6.

2.4. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных является F6 XDR, включающее:

3.2.1. Агенты F6 EDR, установленные на конечные устройства Заказчика, которые проводят:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

3.2.2. F6 NTA, с использованием которого проводится:

- анализ сетевого трафика.
- выявление аномалий, вредоносной активности, скрытых каналов связи и попыток эксплуатации уязвимостей.

3.3. На основе анализа собранных данных автоматически формируются алерты, которые:

- отображаются в Веб-портале F6 XDR в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Обнаруженным алертам автоматически присваиваются следующие статусы:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6.
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенный» или «Ложный»)

4.2. Обнаруженным алертам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.3. F6 вправе корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

5.3. F6 вправе запросить у Заказчика дополнительную информацию для верификации алертов.

5.4. Для верификации алертов могут привлекаться дополнительные программные инструменты F6.

5.5. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза неприменима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

6. УВЕДОМЛЕНИЕ

6.1. При оформлении инцидента F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности;
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.2. В процессе расследования инцидента F6 может дополнять уведомление сведениями, включая:

- информацию о ходе и результатах анализа инцидента;
- дополнительные рекомендации по реагированию на инциденты.

6.3. Порядок направления уведомления:

- для инцидентов среднего уровня — через Веб-портал F6 XDR.
- для инцидентов высокого уровня — через Веб-портал F6 XDR и по телефону или иным способом, согласованным Сторонами.

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается инциденту при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.2. Изменение статусов инцидентов фиксируется в Веб-портале и отражается в отчетности.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Настройка F6 NTA	-	+
Установка агентов F6 EDR	-	+
Мониторинг событий и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10. SLA

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчеты	Оперативный отчет	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.2. УСЛУГА: Комплексный круглосуточный мониторинг и выявление инцидентов ИБ

3.2.1. НАИМЕНОВАНИЕ УСЛУГИ:
Комплексный круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО: F6 ASM и F6 EDR

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования ПО:

- F6 ASM;
- F6 EDR.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного:

- мониторинга и анализа внешней инфраструктуры Заказчика для своевременного выявления инцидентов и предотвращения реализации угроз ИБ;
- выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги F6 осуществляет:

- выявление проблем ИБ на внешних цифровых активах, относящихся к инфраструктуре Заказчика;
- круглосуточный сбор, корреляцию и анализ событий с конечных устройств Заказчика;
- автоматическую классификацию выявленных проблем и событий по уровню критичности (опасности);
- верификацию выявленных проблем и событий ИБ, исследование на предмет компрометации, оформление инцидентов;

- информирование Заказчика об инцидентах;
- формирование рекомендаций по реагированию со стороны Заказчика;
- предоставление отчетов.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются **только** для активов:

- на которых установлены и функционируют агенты F6 EDR, обеспечивающие сбор и передачу телеметрических данных;
- подтвержденных Заказчиком в F6 ASM;

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. Устранение выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по исправлению проблем в рамках данной Услуги.

2.4. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован на активе, который был помечен в Веб-портале F6 ASM Заказчиком как «лишний или игнорируемый».

2.5. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных являются:

3.2.1. Агенты F6 EDR, установленные на конечные устройства Заказчика, которые проводят:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

3.2.2. F6 ASM, которое обеспечивает:

- автоматизированное сканирование внешнего сетевого периметра Заказчика;
- анализ и корреляцию данных для определения критичности (опасности) выявленных проблем.

3.3. Сканирование выполняется без вмешательства в инфраструктуру Заказчика и предназначено для выявления потенциальных уязвимостей, небезопасных конфигураций, а также индикаторов подозрительной или вредоносной активности.

3.4. Политика ответственного сканирования, а также информация о методах и объектах сканирования представлены на сайте https://scan.f6.security/.

3.5. На основе анализа собранных данных автоматически формируются проблемы и алерты, которые:

- отображаются в соответствующих Веб-порталах в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Проблемам, сформированным на основе F6 ASM, автоматически присваивается статус:

Статус	Описание
Обнаруженные	Все обнаруженные проблемы
Решенные	F6 ASM не обнаружило наличие проблемы при повторной проверке

4.2. Проблемам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Критичная опасность	Требует немедленного вмешательства
Высокая опасность	Требует скорейшего вмешательства
Средняя опасность	Требует повышенного внимания
Низкая опасность	Потенциально незначительный ущерб

4.3. Алертам, сформированным на основе F6 EDR, автоматически присваивается статус:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

4.4. Обнаруженным алертам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.5. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. Для F6 ASM:

5.1.1. Анализ проблем со стороны F6 производится только в отношении подтвержденных активов.

5.1.2. Заказчик осуществляет классификацию выявленных активов в Веб-портале F6 ASM, используя статусы:

- «**подтвердить**» – актив принадлежит инфраструктуре Заказчика.
- «**лишние или игнорируемые**» – актив не относится к инфраструктуре Заказчика.

5.1.3. F6 анализирует подтвержденные Проблемы **«Критичного»** и **«Высокого»** уровня по категориям:

- уязвимости;
- сетевая безопасность;
- утечки данных;
- вредоносные программы;
- упоминания в дарквебе.

5.1.4. Анализ проблем «**Среднего**» и «**Низкого**» уровня осуществляется по усмотрению F6.

5.1.5. По результатам верификации F6 устанавливает статус проблемы:

Статус	Описание
Ложно-позитивные	Проблема найдена ошибочно и не подтверждена F6
В работе	Проблема подтверждена, принята в работу F6

5.2. Для F6 EDR:

5.2.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.2.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

5.2.3. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза неприменима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

5.3. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем и алертов.

5.4. Для верификации проблем и алертов могут привлекаться дополнительные программные инструменты F6.

6. УВЕДОМЛЕНИЕ

6.1. При подтверждении проблемы, выявленной с использованием F6 ASM, F6 направляет Заказчику уведомление с указанием:

- краткого описания проблемы;
- списка затронутых активов;
- базовых рекомендаций по устранению проблемы.

6.2. При оформлении инцидента, сформированного на основе алерта в F6 EDR, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности (опасности);
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.3. В процессе расследования F6 дополняет уведомление сведениями о проблеме или инциденте, включая:

- информацию о ходе и результатах анализа проблемы или инцидента;
- дополнительные рекомендации по реагированию на проблему или инцидент.

6.4. Порядок направления уведомления:

Веб-портал	Условие	Способ коммуникации
F6 ASM	Критичная и высокая опасность	Через Веб-портал F6 ASM, по электронной почте или иным способом, согласованным Сторонами
F6 XDR/EDR	Высокая опасность	Через Веб-портал F6 XDR, по электронной почте и по телефону или иным способом, согласованным Сторонами
	Средняя опасность	Через Веб-портал или иным способом, согласованным Сторонами

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается проблеме, выявленной с использованием F6 ASM:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии проблемы при повторном автоматическом сканировании соответствующего актива
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме

7.2. Статус «**Решенный**» присваивается инциденту в F6 EDR при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.3. Изменение статусов проблем и инцидентов фиксируется в соответствующих Веб-порталах и отражается в отчетах.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца:

8.1.1. Ежемесячный отчет о проблемах, выявленных с использованием F6 ASM, включает:

- количество, категории и критичность выявленных проблем;
- перечень активов, на которых обнаружены проблемы;
- принятые меры и оставшиеся риски.

8.1.2. Ежемесячный отчет об инцидентах, выявленных с использованием F6 EDR, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика.

8.2.1. Оперативный отчет о проблеме, выявленной с использованием F6 ASM, включает:

- способ обнаружения проблемы;
- список затронутых активов;
- базовые рекомендации по устранению проблемы;
- рекомендации по локализации инцидента в случае реализации посредством проблемы;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

8.2.2. Оперативный отчет об инциденте, выявленном с использованием F6 EDR, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Сканирование активов и обнаружение проблем	+	-
Подтверждение активов в F6 ASM	-	+
Верификация проблем	+	-
Оповещение	+	-
Устранение проблем	-	+
Установка агентов F6 EDR	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10. SLA

10.1. Целевые показатели, применимые для использования F6 ASM:

Параметр	Условие	Срок
Верификация проблемы	Проблема критического или высокого уровня	До 4 часов
Оповещение Заказчика с предоставлением рекомендаций	Проблема критического или высокого уровня	До 1 часа с момента верификации обнаруженной проблемы
Отчетность	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

10.2. Целевые показатели, применимые для F6 EDR:

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчетность	Отчет об инциденте	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.2.2. НАИМЕНОВАНИЕ УСЛУГИ:
Комплексный круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО: F6 ASM и F6 XDR

11.ОПИСАНИЕ

11.1. Услуга оказывается на основе результатов использования ПО:

- F6 ASM;
- F6 XDR.

11.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

11.3. Услуга направлена на обеспечение непрерывного:

- мониторинга и анализа внешней инфраструктуры Заказчика для своевременного выявления инцидентов и предотвращения реализации угроз ИБ;
- выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

11.4. В рамках оказания Услуги F6 осуществляет:

- выявление проблем ИБ на внешних цифровых активах, относящихся к инфраструктуре Заказчика;
- круглосуточный сбор, корреляция и анализ событий ИБ с конечных устройств и сетевой инфраструктуры Заказчика;
- автоматическая классификация выявленных проблем и событий по уровню критичности (опасности);
- верификация выявленных проблем и событий ИБ, исследование на предмет компрометации, оформление инцидентов;
- информирование Заказчика об Инцидентах;
- формирование рекомендаций по реагированию со стороны Заказчика;
- подготовка отчетов.

12. ОБЛАСТЬ ПРИМЕНЕНИЯ

12.1. Услуги оказываются **только** для активов:

- на которых установлены и функционируют агенты F6 EDR, обеспечивающие сбор и передачу телеметрических данных;
- находящихся в сетевых сегментах, трафик с которых поступает в F6 NTA;
- подтвержденных Заказчиком в F6 ASM;

12.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

12.3. Исправление выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по исправлению проблем в рамках данной Услуги.

12.4. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован на активе, который был помечен в Веб-портале F6 ASM Заказчиком как «лишний или игнорируемый».

12.5. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

13. СБОР И ОБРАБОТКА ДАННЫХ

13.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

13.2. Источником сбора данных являются:

13.2.1. F6 XDR, включающее:

13.2.1.1. Агенты F6 EDR, установленные на конечные устройства Заказчика, которые проводят:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

13.2.1.2. F6 NTA, с использованием которого осуществляется:

- анализ сетевого трафика;
- выявление аномалий, вредоносной активности, скрытых каналов связи и попыток эксплуатации уязвимостей.

13.2.2. F6 ASM, которое обеспечивает:

- автоматизированное сканирование внешнего сетевого периметра Заказчика;
- анализ и корреляцию данных для определения критичности (опасности) выявленных проблем.

13.3. Сканирование выполняется без вмешательства в инфраструктуру Заказчика и предназначено для выявления потенциальных уязвимостей, небезопасных конфигураций, а также индикаторов подозрительной или вредоносной активности.

13.4. Политика ответственного сканирования, а также информация о методах и объектах сканирования представлены на сайте https://scan.f6.security/.

13.5. На основе анализа собранных данных автоматически формируются проблемы и алерты, которые:

- отображаются в соответствующих Веб-порталах в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

14. КЛАССИФИКАЦИЯ

14.1. Проблемам, сформированным с использованием F6 ASM, автоматически присваивается статус:

Статус	Описание
Обнаруженные	Все обнаруженные проблемы
Решенные	F6 ASM не обнаружило наличие проблемы при повторной проверке

14.2. Проблемам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Критичная опасность	Требует немедленного вмешательства
Высокая опасность	Требует скорейшего вмешательства
Средняя опасность	Требует повышенного внимания
Низкая опасность	Потенциально незначительный ущерб

14.3. Алертам, сформированным с использованием F6 XDR, автоматически присваивается статус:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

14.4. Обнаруженным алертам автоматически присваивается уровень опасности:

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

14.5. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

15. АНАЛИЗ И ВЕРИФИКАЦИЯ

15.1. Для F6 ASM:

15.1.1. Анализ проблем со стороны F6 производится только в отношении **подтвержденных** активов.

15.1.2. Заказчик осуществляет классификацию выявленных активов в Веб-портале F6 ASM, используя статусы:

- «**подтвердить**» – актив принадлежит инфраструктуре Заказчика.
- «**лишние или игнорируемые**» – актив не относится к инфраструктуре Заказчика.

15.1.3. F6 анализирует подтвержденные проблемы **«Критичного»** и **«Высокого»** уровня по категориям:

- уязвимости;
- сетевая безопасность;
- утечки данных;
- вредоносные программы;
- упоминания в дарквебе.

15.1.4. Анализ проблем «**Среднего**» и «**Низкого**» уровня осуществляется по усмотрению F6.

15.1.5. По результатам верификации F6 устанавливает статус проблемы:

Статус	Описание
Ложно-позитивные	Проблема найдена ошибочно и не подтверждена F6
В работе	Проблема подтверждена, принята в работу F6

15.2. Для F6 XDR:

15.2.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

15.2.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

15.2.3. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события ИБ отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза неприменима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

15.3. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем и алертов.

15.4. Для верификации проблем и алертов могут привлекаться дополнительные программные инструменты F6.

16. УВЕДОМЛЕНИЕ

16.1. При подтверждении проблемы, выявленной с использованием F6 ASM, F6 направляет Заказчику уведомление с указанием:

- краткого описания проблемы;
- списка затронутых активов;
- базовых рекомендаций по устранению проблемы.

16.2. При оформлении инцидента, сформированного на основе алерта в F6 XDR, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности;
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

16.3. В процессе расследования F6 дополняет сведения о проблеме или инциденте, включая:

- информацию о ходе и результатах анализа проблемы или инцидента;
- дополнительные рекомендации по реагированию на проблему или инцидент.

16.4. Порядок информирования:

Веб-портал	Условие	Способ коммуникации
F6 ASM	Критичная и высокая опасность	Через Веб-портал F6 ASM, по электронной почте или иным способом, согласованным Сторонами
F6 XDR/EDR	Высокая опасность	Через Веб-портал F6 XDR, по электронной почте и по телефону или иным способом, согласованным Сторонами
	Средняя опасность	Через Веб-портал F6 XDR или иным способом, согласованным Сторонами

17. РЕШЕНИЕ

17.1. Статус «**Решенный**» присваивается проблеме, выявленной с использованием F6 ASM:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии проблемы при повторном автоматическом сканировании соответствующего актива
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме

17.2. Статус «**Решенный**» присваивается инциденту в F6 XDR при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

17.3. Изменение статусов проблем и инцидентов фиксируется в соответствующих Веб-порталах и отражается в отчетах.

18. ОТЧЕТЫ

18.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца:

18.1.1. Ежемесячный отчет о проблемах, выявленных с использованием F6 ASM, включает:

- количество, категории и критичность выявленных проблем;

- перечень активов, на которых они обнаружены;
- принятые меры и оставшиеся риски.

18.1.2. Ежемесячный отчет об инцидентах, выявленных с использованием F6 XDR, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

18.2. Оперативный отчет предоставляется по запросу Заказчика:

18.2.1. Оперативный отчет о проблеме, выявленной с использованием F6 ASM, включает:

- способ обнаружения проблемы;
- список затронутых активов;
- базовые рекомендации по устранению проблемы;
- рекомендации по локализации инцидента в случае реализации посредством проблемы;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

18.2.2. Оперативный отчет об инциденте, выявленном с использованием F6 XDR, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

19. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Сканирование активов и обнаружение проблем	+	-
Подтверждение активов в F6 ASM	-	+
Верификация проблем	+	-
Оповещение	+	-
Устранение проблем	-	+
Настройка F6 NTA	-	+
Установка агентов F6 EDR	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

20. SLA

20.1. Целевые показатели, применимые для использования F6 ASM:

Параметр	Условие	Срок
Верификация проблемы	Проблема критического или высокого уровня	До 4 часов
Оповещение Заказчика с предоставлением рекомендаций	Проблема критического или высокого уровня	До 1 часа с момента верификации обнаруженной проблемы
Отчеты	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

20.2. Целевые показатели, применимые для использования F6 XDR:

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчетность	Отчет об инциденте	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.2.3. НАИМЕНОВАНИЕ УСЛУГИ:
Комплексный круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО: F6 ASM, F6 EDR и SIEM

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования ПО:

- F6 ASM;
- F6 EDR;
- SIEM.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного:

- мониторинга и анализа внешней инфраструктуры Заказчика для своевременного выявления инцидентов и предотвращения реализации угроз ИБ;
- выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги осуществляется:

- выявление проблем ИБ на внешних цифровых активах, относящихся к инфраструктуре Заказчика;
- сбор, нормализация и корреляция событий ИБ от подключенных источников;
- автоматическая классификация выявленных проблем и событий ИБ по уровню критичности (опасности);
- верификация выявленных проблем и событий ИБ, исследование на предмет компрометации, оформление инцидентов;
- информирование Заказчика об инцидентах;

- формирование рекомендаций по реагированию со стороны Заказчика;
- подготовка отчетов.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются **только** для активов:

- на которых установлены и функционируют агенты F6 EDR, обеспечивающие сбор и передачу телеметрических данных;
- подтвержденных Заказчиком в F6 ASM;
- с которых события ИБ поступают в SIEM:
  - активы как прямой источник событий;
  - активы, охваченные мониторингом посредством другого источника, подключенного к SIEM.

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. Устранение выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по исправлению проблем в рамках данной Услуги.

2.4. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован на активе, который был помечен в Веб-портале F6 ASM Заказчиком как «лишний или игнорируемый».

2.5. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных являются:

3.2.1. Агенты F6 EDR, установленные на конечные устройства, которые проводят:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

3.2.2. F6 ASM, которое обеспечивает:

- автоматизированное сканирование внешнего сетевого периметра Заказчика;
- анализ и корреляцию данных для определения критичности выявленных проблем.

3.2.3. SIEM, которая обеспечивает:

- сбор и анализ (корреляцию) информации о событиях ИБ с источников, не включенных в область мониторинга F6 EDR;
- обогащение инцидентов дополнительным контекстом.

3.3. Сканирование выполняется без вмешательства в инфраструктуру Заказчика и предназначено для выявления потенциальных уязвимостей, небезопасных конфигураций, а также индикаторов подозрительной или вредоносной активности.

3.4. Политика ответственного сканирования, а также информация о методах и объектах сканирования представлены на сайте https://scan.f6.security/.

3.5. На основе анализа собранных данных автоматически формируются проблемы и алерты, которые:

- отображаются в соответствующих Веб-порталах в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Проблемам, сформированным с использованием F6 ASM, автоматически присваивается статус:

Статус	Описание
Обнаруженные	Все обнаруженные проблемы
Решенные	F6 ASM не обнаружило наличие проблемы при повторной проверке

4.2. Проблемам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Критичная опасность	Требует немедленного вмешательства
Высокая опасность	Требует скорейшего вмешательства
Средняя опасность	Требует повышенного внимания
Низкая опасность	Потенциально незначительный ущерб

4.3. Алертам, сформированным с использованием F6 EDR, автоматически присваивается статус:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

4.4. Обнаруженным алертам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.5. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. Для F6 ASM:

5.1.1. Анализ проблем со стороны F6 производится только в отношении **подтвержденных** активов.

5.1.2. Заказчик осуществляет классификацию выявленных активов в Веб-портале F6 ASM, используя статусы:

- «**подтвердить**» – актив принадлежит инфраструктуре Заказчика;
- «**лишние или игнорируемые**» – актив не относится к инфраструктуре Заказчика.

5.1.3. F6 анализирует подтвержденные проблемы **«Критичного»** и **«Высокого»** уровня по категориям:

- уязвимости;
- сетевая безопасность;
- утечки данных;
- вредоносные программы;
- упоминания в дарквебе.

5.1.4. Анализ проблем «**Среднего**» и «**Низкого**» уровня осуществляется по усмотрению F6.

5.1.5. По результатам верификации F6 устанавливает статус проблемы:

Статус	Описание
Ложно-позитивные	Проблема найдена ошибочно и не подтверждена F6
В работе	Проблема подтверждена, принята в работу F6

5.2. Для F6 EDR:

5.2.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.2.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6

5.2.3. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события ИБ отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза не применима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

5.3. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем и алертов.

5.4. Для верификации проблем и алертов могут привлекаться дополнительные программные инструменты F6.

6. УВЕДОМЛЕНИЕ

6.1. При подтверждении проблемы, выявленной с использованием F6 ASM, F6 направляет Заказчику уведомление с указанием:

- краткого описания проблемы;
- списка затронутых активов;
- базовых рекомендаций по устранению проблемы.

6.2. При оформлении инцидента, сформированного на основе алерта в F6 EDR, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности (опасности);
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.3. В процессе расследования F6 дополняет уведомление сведениями о проблеме или инциденте, включая:

- информацию о ходе и результатах анализа проблемы или инцидента;
- дополнительные рекомендации по реагированию на проблему или инцидент.

6.4. Порядок информирования:

Веб-портал	Условие	Способ коммуникации
F6 ASM	Критичная и высокая опасность	Через Веб-портал F6 ASM, по электронной почте или иным способом, согласованным Сторонами
F6 XDR/EDR	Высокая опасность	Через Веб-портал F6 XDR, по электронной почте и по телефону или иным способом, согласованным Сторонами
	Средняя опасность	Через Веб-портал F6 XDR или иным способом, согласованным Сторонами

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается проблеме, выявленной с использованием F6 ASM:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии проблемы при повторном автоматическом сканировании соответствующего актива
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме

7.2. Статус «**Решенный**» присваивается инциденту в F6 EDR при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.3. Изменение статусов проблем и инцидентов фиксируется в соответствующих Веб-порталах и отражается в отчетах.

8. ОТЧЕТНОСТЬ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца.

8.1.1. Ежемесячный отчет о проблемах, выявленных с использованием F6 ASM, включает:

- количество, категории и критичность выявленных проблем;
- перечень активов, на которых обнаружены проблемы;
- принятые меры и оставшиеся риски.

8.1.2. Ежемесячный отчет об инцидентах, выявленных с использованием F6 EDR, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика:

8.2.1. Оперативный отчет о проблеме, выявленной F6 ASM, включает:

- способ обнаружения проблемы;
- список затронутых активов;
- базовые рекомендации по устранению проблемы;
- рекомендации по локализации инцидента в случае реализации посредством проблемы;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

8.2.2. Оперативный отчет об инциденте, выявленном с использованием F6 EDR, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Сканирование активов и обнаружение проблем	+	-
Подтверждение активов в F6 ASM	-	+
Верификация проблем	+	-
Подключение источников к SIEM	+	-
Оповещение	+	-
Устранение проблем	-	+
Установка агентов F6 EDR	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10. SLA

10.1. Целевые показатели, применимые для F6 ASM:

Параметр	Условие	Срок
Верификация проблемы	Проблема критического или высокого уровня	До 4 часов
Оповещение Заказчика с предоставлением рекомендаций	Проблема критического или высокого уровня	До 1 часа с момента верификации обнаруженной проблемы
Отчет	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

10.2. Целевые показатели, применимые для F6 EDR:

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчет	Отчет об инциденте	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.2.4. НАИМЕНОВАНИЕ УСЛУГИ:
Комплексный круглосуточный мониторинг и выявление инцидентов ИБ с использованием ПО: F6 ASM, F6 XDR и SIEM

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования ПО:

- F6 ASM;
- F6 XDR;
- SIEM.

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на обеспечение непрерывного:

- мониторинга и анализа внешней инфраструктуры Заказчика для своевременного выявления инцидентов и предотвращения реализации угроз ИБ;
- выявления киберугроз и предоставления рекомендаций по реагированию с целью минимизации воздействия инцидентов.

1.4. В рамках оказания Услуги осуществляется:

- выявление проблем ИБ на внешних цифровых активах, относящихся к инфраструктуре Заказчика;
- сбор, нормализация и корреляция событий ИБ от подключенных источников;
- автоматическая классификация выявленных проблем и событий ИБ по уровню критичности (опасности);
- верификация выявленных проблем и событий ИБ, исследование на предмет компрометации, оформление инцидентов;

- информирование Заказчика об инцидентах;
- формирование рекомендаций по реагированию со стороны Заказчика;
- подготовка отчетов.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются **только** для активов:

- на которых установлены и функционируют агенты F6 EDR, обеспечивающие сбор и передачу телеметрических данных;
- находящихся в сетевых сегментах, трафик с которых поступает в F6 NTA;
- подтвержденных Заказчиком в F6 ASM;
- с которых события безопасности поступают в SIEM:
  - активы как прямой источник событий ИБ;
  - активы, охваченные мониторингом посредством другого источника, подключенного к SIEM.

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. Исправление выявленных проблем выполняется Заказчиком, F6 не осуществляет действий по устранению проблем в рамках данной Услуги.

2.4. F6 не несет ответственности за любой ущерб, возникший в рамках инцидента, который:

- был реализован на активе, не включенном в область применения Услуги;
- был выявлен в рамках Услуги, но по которому отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;

- был реализован через выявленную проблему, по которой отсутствовала соответствующая реакция со стороны Заказчика, в том числе не были вовремя предприняты рекомендации, предоставленные F6;
- был реализован на активе, который был помечен в Веб-портале F6 ASM Заказчиком как «лишний или игнорируемый».

2.5. В случае, если Заказчиком приобретена Услуга по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инцидент.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных являются:

3.2.1. F6 XDR, которое включает:

3.2.1.1. Агенты F6 EDR, установленные на конечные устройства Заказчика, который проводят:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

3.2.1.2. F6 NTA, с использованием которого проводится:

- анализ сетевого трафика;
- выявление аномалий, вредоносной активности, скрытых каналов связи и попыток эксплуатации уязвимостей.

3.2.2. F6 ASM, которое обеспечивает:

- автоматизированное сканирование внешнего сетевого периметра Заказчика;
- анализ и корреляцию данных для определения критичности выявленных проблем.

3.2.3. SIEM, которая обеспечивает:

- сбор и анализ (корреляцию) информации о событиях ИБ с источников, не включенных в область мониторинга F6 XDR;
- обогащение инцидентов дополнительным контекстом.

3.3. Сканирование выполняется без вмешательства в инфраструктуру Заказчика и предназначено для выявления потенциальных уязвимостей, небезопасных конфигураций, а также индикаторов подозрительной или вредоносной активности.

3.4. Политика ответственного сканирования, а также информация о методах и объектах сканирования представлены на сайте https://scan.f6.security/.

3.5. На основе анализа собранных данных автоматически формируются проблемы и алерты, которые:

- отображаются в соответствующих Веб-порталах в режиме реального времени;
- автоматически классифицируются по уровню критичности (опасности);
- направляются на дальнейший анализ специалистами F6.

4. КЛАССИФИКАЦИЯ

4.1. Проблемам, сформированным с использованием F6 ASM, автоматически присваивается статус:

Статус	Описание
Обнаруженные	Все обнаруженные проблемы
Решенные	F6 ASM не обнаружило наличие проблемы при повторной проверке

4.2. Проблемам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Критичная опасность	Требует немедленного вмешательства
Высокая опасность	Требует скорейшего вмешательства
Средняя опасность	Требует повышенного внимания
Низкая опасность	Потенциально незначительный ущерб

4.3. Алертам, сформированным с использованием F6 XDR, автоматически присваивается статус:

Статус	Описание
Новые	Алерты, которые не соответствуют критериям для автоматической обработки в соответствии с настроенными правилами F6
Закрытые	Алерты, автоматически обработанные системой на основании выполнения заданных F6 критериев для закрытия (в соответствии с правилами автоматического назначения статуса «Решенные»)

4.4. Обнаруженным алертам автоматически присваивается уровень критичности (опасности):

Уровень	Описание
Высокий	Подтвержденное вредоносное воздействие, успешная эксплуатация критичных уязвимостей, заражение устройства
Средний	Подозрительные аномалии в поведении систем или сети, попытки эксплуатации уязвимостей
Низкий	Некритичная активность, требующая наблюдения

4.5. F6 имеет право корректировать уровень критичности (опасности) с учетом динамики угроз.

5. АНАЛИЗ И ВЕРИФИКАЦИЯ

5.1. Для F6 ASM:

5.1.1. Анализ проблем со стороны F6 производится только в отношении **подтвержденных** активов.

5.1.2. Заказчик осуществляет классификацию выявленных активов в Веб-портале F6 ASM, используя статусы:

- «**подтвердить**» – актив принадлежит инфраструктуре Заказчика;
- «**лишние или игнорируемые**» – актив не относится к инфраструктуре Заказчика.

5.1.3. F6 анализирует подтвержденные проблемы **«Критичного»** и **«Высокого»** уровня по категориям:

- уязвимости;
- сетевая безопасность;
- утечки данных;
- вредоносные программы;
- упоминания в дарквебе.

5.1.4. Анализ проблем «**Среднего**» и «**Низкого**» уровня осуществляется по усмотрению F6.

5.1.5. По результатам верификации F6 устанавливает статус проблемы:

Статус	Описание
Ложно-позитивные	Проблема найдена ошибочно и не подтверждена F6
В работе	Проблема подтверждена, принята в работу F6

5.2. Для F6 XDR:

5.2.1. F6 анализирует **новые** алерты с уровнем «**Высокий**» и «**Средний**».

5.2.2. Анализ алертов «**Низкого**» уровня осуществляется по усмотрению F6.

5.2.3. По результатам анализа каждому алерту присваивается один из следующих статусов:

Статус	Описание
Ложно-положительный	Срабатывание сигнатуры/правила некорректно, вредоносная активность отсутствует; события ИБ отнесены к легитимной активности Заказчика
Решенный	Сигнатура сработала корректно, но угроза неприменима к инфраструктуре или активам Заказчика (например: эксплуатация уязвимости невозможна в конкретной конфигурации)
Инцидент	Подтвержденная вредоносная активность, атака или эксплуатация уязвимости, требующая принятия мер реагирования

5.3. F6 вправе запрашивать у Заказчика дополнительные данные, необходимые для верификации проблем и алертов.

5.4. Для верификации проблем и алертов могут привлекаться дополнительные программные инструменты F6.

6. УВЕДОМЛЕНИЕ

6.1. При подтверждении проблемы, выявленной с использованием F6 ASM, F6 направляет Заказчику уведомление с указанием:

- краткого описания проблемы;
- списка затронутых активов;
- базовых рекомендаций по устранению проблемы.

6.2. При оформлении инцидента, сформированного на основе алерта в F6 XDR, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности;
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

6.3. В процессе расследования F6 дополняет сведения о проблеме или инциденте, включая:

- информацию о ходе и результатах анализа;
- дополнительные рекомендации по реагированию.

6.4. Порядок информирования:

Веб-портал	Условие	Способ коммуникации
F6 ASM	Критичная и высокая опасность	Через Веб-портал, по электронной почте или иным способом, согласованным Сторонами
F6 XDR/EDR	Высокая опасность	Через Веб-портал, по электронной почте и по телефону или иным способом, согласованным Сторонами
	Средняя опасность	Через Веб-портал или иным способом, согласованным Сторонами

7. РЕШЕНИЕ

7.1. Статус «**Решенный**» присваивается проблеме, выявленной с использованием F6 ASM:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии проблемы при повторном автоматическом сканировании соответствующего актива
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме

7.2. Статус «**Решенный**» присваивается инциденту в F6 XDR при следующих условиях:

Способ присвоения статуса	Условия присвоения статуса «Решенный»
Автоматически	При отсутствии признаков продолжающейся вредоносной активности, связанной с данным инцидентом, в течение 10 календарных дней с момента последней зафиксированной активности и при отсутствии обратной связи от Заказчика за указанный период
Вручную F6	При получении от Заказчика обратной связи, подтверждающей успешное выполнение рекомендаций F6 в полном объеме
	При подтверждении F6 отсутствия признаков продолжающейся вредоносной активности, связанной с данным инцидентом, на основе данных мониторинга

7.3. Изменение статусов проблем и инцидентов фиксируется в соответствующих Веб-порталах и отражается в отчетах.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца:

8.1.1. Ежемесячный отчет о проблемах, выявленных с использованием F6 ASM, включает:

- количество, категории и критичность выявленных проблем;
- перечень активов, на которых обнаружены проблемы;
- принятые меры и оставшиеся риски.

8.1.2. Ежемесячный отчет об инцидентах, выявленных с использованием F6 XDR, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

8.2. Оперативный отчет предоставляется по запросу Заказчика:

8.2.1. Оперативный отчет о проблеме, выявленной с использованием F6 ASM, включает:

- способ обнаружения проблемы;
- список затронутых активов;
- базовые рекомендации по устранению проблемы;
- рекомендации по локализации инцидента, в случае реализации посредством проблемы;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

8.2.2. Оперативный отчет об инциденте, выявленном с использованием F6 XDR, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Сканирование активов и обнаружение Проблем	+	-
Подтверждение активов в F6 ASM	-	+
Верификация Проблем	+	-
Подключение источников к SIEM	+	-
Оповещение	+	-
Устранение Проблем	-	+
Настройка F6 NTA	-	+
Установка агентов F6 EDR	-	+
Мониторинг событий ИБ и алертов	+	-
Верификация алертов	+	-
Оформление инцидентов	+	-
Оповещение с рекомендациями	+	-
Реагирование и нейтрализация	-	+

10. SLA

10.1. Целевые показатели, применимые для F6 ASM:

Параметр	Условие	Срок
Верификация Проблемы	Проблема критического или высокого уровня	До 4 часов
Оповещение Заказчика с предоставлением рекомендаций	Проблема критического или высокого уровня	До 1 часа с момента верификации обнаруженной Проблемы
Отчет	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

10.2. Целевые показатели, применимые для F6 XDR:

Параметр	Условие	Срок
Валидация алерта	Алерт высокого уровня опасности	До 30 минут
	Алерт среднего уровня опасности	До 60 минут
Оповещение о подтвержденном инциденте с рекомендациями	-	До 60 минут с момента генерации первого алерта, формирующего инцидент
Отчетность	Отчет об инциденте	До 48 часов с момента запроса
	Ежемесячный отчет	В течение 10 рабочих дней с даты окончания календарного месяца

3.3. УСЛУГА: Оперативное реагирование на выявленные инциденты ИБ

3.3.1. НАИМЕНОВАНИЕ УСЛУГИ:
Оперативное реагирование на выявленные инциденты ИБ с использованием ПО: F6 EDR ИЛИ F6 XDR

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования F6 EDR (предоставляемого отдельно или в составе F6 XDR) и предоставляется исключительно **при условии** оказания Заказчику Услуги «Круглосуточный мониторинг и выявление инцидентов ИБ» или «Комплексный круглосуточный мониторинг и выявление инцидентов ИБ».

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга заключается в оперативном реагировании на подтвержденные инциденты ИБ путем выполнения активных действий на конечных устройствах инфраструктуры Заказчика с использованием функциональных возможностей F6 EDR.

1.4. Основные направления предоставления Услуги:

- локализация инцидентов ИБ (изоляция скомпрометированных устройств);
- сбор и анализ цифровых артефактов;
- проведение мероприятий по устранению угроз и восстановлению ИБ.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются только для активов, на которых установлены и функционируют агенты F6 EDR.

2.2. Реагирование осуществляется в рамках подтвержденных инцидентов ИБ, выявленных в процессе оказания Услуги «Круглосуточный мониторинг и выявление инцидентов ИБ» или «Комплексный круглосуточный мониторинг и выявление инцидентов ИБ».

3. ОСНОВАНИЯ ДЛЯ РЕАГИРОВАНИЯ

3.1. Активное реагирование инициируется при выполнении одного из условий:

- обоснованное подозрение со стороны F6 на реализацию инцидента ИБ;
- подтверждение инцидента ИБ со стороны F6;
- мотивированный запрос от представителя Заказчика, направленный в установленном порядке.

4. АКТИВНЫЕ ДЕЙСТВИЯ

4.1. В целях предотвращения распространения угрозы и минимизации потенциального ущерба F6 уполномочен предпринимать следующие меры без получения дополнительного согласования Заказчика:

- принудительная сетевая изоляция устройств, вовлеченных в инцидент. Изоляция осуществляется средствами агента F6 EDR и может включать блокировку сетевых подключений, за исключением служебных каналов, необходимых для функционирования F6 EDR;
- криминалистическое исследование и сбор цифровых артефактов с устройств, непосредственно задействованных в инциденте, а также со смежных систем и источников данных инфраструктуры Заказчика.

5. УВЕДОМЛЕНИЕ

5.1. F6 уведомляет Заказчика в течение 15 минут после применения мер реагирования.

5.2. Информирование осуществляется через Веб-портал и по телефону/согласованным каналам связи.

5.3. Уведомление содержит:

- краткое описание инцидента;
- наименование и идентификаторы изолированного устройства;
- оперативные рекомендации.

6. ИССЛЕДОВАНИЕ

6.1. F6 осуществляет сбор криминалистически значимых данных задействованных в инциденте устройств с использованием встроенных сценариев F6 EDR.

6.2. При невозможности автоматического сбора данных F6 направляет Заказчику детализированные инструкции для самостоятельного сбора данных.

6.3. По результатам анализа F6:

- реконструирует ход инцидента;
- определяет масштаб компрометации;
- формирует дополнительные рекомендации.

7. ВОССТАНОВЛЕНИЕ

7.1. После локализации инцидента, по согласованию с Заказчиком выполняются мероприятия по восстановлению, включая:

- удаление вредоносных компонентов и артефактов;
- блокировку вредоносных локальных учетных записей;
- корректировку настроек политик безопасности.

7.2. Мероприятия восстановления ограничиваются функциональными возможностями F6 EDR.

8. ПРОЦЕДУРА ВОЗВРАТА В ЭКСПЛУАТАЦИЮ

8.1. По завершении мероприятий по нейтрализации угроз и восстановлению, F6 инициирует процедуру возврата устройств в производственную среду Заказчика. Возврат устройства осуществляется поэтапно:

8.1.1. Верификация результатов восстановления – F6 проводит финальную проверку устройства на отсутствие признаков компрометации и подтверждает готовность к возврату в эксплуатацию.

8.1.2. Снятие ограничений – F6 осуществляет снятие ранее примененных мер изоляции.

9. ОТЧЕТЫ

9.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца, включает:

- статистику инцидентов;
- категории и типы угроз;
- краткое описание инцидентов.

9.2. Оперативный отчет предоставляется по запросу Заказчика, включает:

- способ обнаружения инцидента;
- хронологию инцидента;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

10. РЕШЕНИЕ

10.1. Инциденту присваивается Статус «**Решенный**» после успешного выполнения комплекса мероприятий по его локализации, восстановлению и возврату в эксплуатацию.

10.2. Изменение статусов инцидентов фиксируется в Веб-портале и отражается в отчете.

11. RACI-МАТРИЦА

Процесс/Операция	F6	Заказчик
Инициация реагирования на инцидент	+	+
Принятие решения об изоляции устройств	+	-
Криминалистический анализ и расследование	+	-
Выполнение работ по восстановлению	+	-
Принятие решения о возврате устройств в эксплуатацию	+	-
Закрытие инцидента	+	-
Реализация рекомендаций по повышению защищенности	-	-

12. SLA

Параметр	Условие	Срок
Локализация устройства	Инцидент, на основе алертов высокой опасности	До 60 минут с момента генерации алерта, на основе которого будет сформирован инцидент
Оповещение Заказчика	После применения мер реагирования	До 15 минут
Мероприятия по восстановлению	После согласования с Заказчиком	До 48 часов
Отчет об инциденте	После применения мер восстановления	До 48 часов
Регулярный отчет	Ежемесячно	В течение 10 рабочих дней по окончании календарного месяца

3.4. УСЛУГА: Проактивный поиск недетектируемых угроз

3.4.1. НАИМЕНОВАНИЕ УСЛУГИ: Проактивный поиск недетектируемых угроз с использованием ПО: F6 EDR ИЛИ F6 XDR

1. ОПИСАНИЕ

1.1. Услуга оказывается на основе результатов использования F6 EDR (предоставляемого отдельно или в составе F6 XDR) и предоставляется исключительно **при условии** оказания Заказчику Услуги «Круглосуточный мониторинг и выявление инцидентов ИБ» или «Комплексный круглосуточный мониторинг и выявление инцидентов ИБ».

1.2. Услуга оказывается специалистами F6 удаленно, в круглосуточном режиме.

1.3. Услуга направлена на выявление скрытых, сложных и ранее неизвестных угроз ИБ, которые не обнаруживаются стандартными автоматизированными средствами и правилами корреляции.

1.4. В рамках Услуги F6 осуществляет:

- ретроспективный анализ телеметрических данных, собранных с использованием F6 EDR;
- выявление следов компрометации инфраструктуры Заказчика.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Услуги оказываются только для активов, на которых установлены и функционируют агенты F6 EDR.

2.2. Реагирование на инциденты выполняется Заказчиком, F6 не осуществляет действий по устранению угроз в рамках данной Услуги.

2.3. В случае, если Сертификат включает Услугу по оперативному реагированию на выявленные инциденты ИБ, F6 вправе приступить к реагированию на соответствующий инциденты.

3. СБОР И ОБРАБОТКА ДАННЫХ

3.1. Сбор данных осуществляется исключительно в целях оказания Услуги.

3.2. Источником сбора данных является агент F6 EDR, установленный на конечные устройства Заказчика, который проводит:

- сбор событий операционных систем и пользовательской активности;
- мониторинг процессов, файловых операций и сетевых соединений на уровне устройства;
- выявление попыток компрометации и вредоносного поведения.

4. ПРОВЕДЕНИЕ ПОИСКОВЫХ ОПЕРАЦИЙ

4.1. F6 осуществляет постоянный сбор и систематизацию данных об актуальных угрозах, информацию о которых F6 получает на регулярной основе из публичных и не публичных источников в рамках процесса киберразведки.

4.2. На основе анализа актуальных угроз и с учетом особенностей инфраструктуры Заказчика формируются гипотезы компрометации – специализированные запросы к телеметрическим данным, собранными агентами F6 EDR с конечных устройств Заказчика.

4.3. Глубина исторического поиска ограничена сроком хранения телеметрических данных.

5. ЗАПРОСЫ НА ПРОВЕРКУ ГИПОТЕЗ

5.1. Заказчик вправе инициировать мотивированный запрос на проверку гипотезы компрометации, предоставив F6 обоснование, включающее:

- описание подозрительной активности или аномалии;
- конкретные индикаторы компрометации (IoC) для проверки;
- временные рамки исследуемого периода;
- область поиска (определенные сегменты инфраструктуры, группы пользователей или систем).

5.2. F6 обязан принять заявку Заказчика и реализовать проверку гипотезы в установленные сроки.

5.3. Количество индивидуальных запросов Заказчика ограничено **пятью запросами** в течение календарного месяца.

5.4. Запросы, превышающие установленный лимит, могут быть приняты к рассмотрению по отдельному согласованию Сторон.

5.5. Срок выполнения проверки гипотезы по индивидуальному запросу Заказчика составляет **не более 48 часов** с момента получения F6 мотивированного запроса, оформленного надлежащим образом. Отсчет времени выполнения начинается с момента получения F6 полного объема информации, необходимой для проведения проверки.

5.6. В случае, если для проверки гипотезы требуется дополнительная информация от Заказчика, срок выполнения может быть приостановлен до момента получения запрашиваемых данных.

6. ИССЛЕДОВАНИЕ И КЛАССИФИКАЦИЯ

6.1. F6 проводит детальный анализ всех событий ИБ, соответствующих условиям поиска, с целью идентификации подозрительной активности.

6.2. Для подтверждения гипотез используются:

- сравнение с известными индикаторами компрометации (IoCs);
- статический и поведенческий анализ подозрительных объектов;
- корреляция с другими событиями ИБ, свидетельствующими о вредоносном поведении.

6.3. F6 вправе связаться с Заказчиком и запросить дополнительные данные, необходимые для оценки событий ИБ.

6.4. F6 вправе инициировать сбор дополнительных цифровых артефактов с устройства с целью оценки событий ИБ.

7. УВЕДОМЛЕНИЕ ЗАКАЗЧИКА

7.1. В случае, если выявленные события ИБ признаны вредоносными, F6 направляет Заказчику уведомление с указанием:

- описания инцидента и его критичности;
- первичных рекомендаций по оперативным действиям с целью устранения угрозы.

7.2. В процессе расследования F6 может дополнять сведения, включая:

- информацию о ходе и результатах анализа;
- дополнительные рекомендации по реагированию.

7.3. Информирование осуществляется через Веб-портал и/или иным способом, согласованным Сторонами.

8. ОТЧЕТЫ

8.1. Ежемесячный отчет предоставляется в течение 10 рабочих дней после окончания календарного месяца, включает:

- статистику по поисковым запросам;
- информацию о новых техниках, поиск которых реализован за отчетный период;
- описание выявленных угроз и ответных действий.

8.2. Оперативный отчет предоставляется по запросу Заказчика, включает:

- способ обнаружения угрозы;
- хронологию развития атаки;
- предоставленные F6 рекомендации по локализации и восстановлению;
- перечень выявленных индикаторов компрометации (IoC);
- рекомендации по повышению защищенности.

9. SLA

Параметр	Срок
Проверка гипотез по индивидуальному запросу Заказчика	До 48 часов
Ежемесячный отчет о результатах поиска	В течение 10 рабочих дней с даты окончания календарного месяца
Оперативный отчет	До 48 часов с момента запроса Заказчика

4 ОТВЕТСТВЕННОСТЬ F6 ЗА НАРУШЕНИЕ SLA

4.1. Основания для признания нарушения SLA:

4.1.1. Нарушением SLA признается превышение целевых сроков, установленных в разделах SLA настоящих Специальных условий, при обработке одной проблемы или одного инцидента. Нарушение считается подтвержденным, если превышение составляет более 30% от установленного в SLA срока.

4.2. Исключения, не признаваемые нарушением SLA:

4.2.1. Не классифицируются как нарушение SLA случаи, когда превышение сроков произошло по следующим причинам:

- алерт был добавлен в существующий инцидент, и его добавление не повлияло на ход расследования;
- проведение планового или экстренного обслуживания ПО, используемого для оказания Услуг;
- нарушение работоспособности оборудования или недоступность данных на стороне Заказчика.

4.3. Порядок расчета компенсации:

4.3.1. При подтверждении нарушения SLA F6 предоставляет Заказчику компенсацию, рассчитываемую по формуле:

Компенсация = Вознаграждение за оказание Услуг (передачу Сертификата), полученное F6 от Заказчика или Партнера, в рамках срока их оказания (срока его действия) × K,

*где **K** = (Количество инцидентов/проблем с нарушением SLA в рамках срока оказания Услуг (срока действия Сертификата)) / (Общее количество инцидентов/проблем за тот же период).*

4.4. Условия предоставления компенсации:

4.4.1. Компенсация предоставляется в виде скидки при последующем приобретении Услуг (Сертификата), оказываемых (реализуемых) F6.

4.4.2. Максимальный размер компенсации не может превышать 10% от вознаграждения F6, полученного от Заказчика или Партнера, за оказание Услуг (передачу Сертификата), в рамках оказания которых (срока действия которого) было зафиксировано нарушение SLA.

4.4.3. Для получения компенсации Заказчик обязан направить мотивированный запрос с документальным подтверждением нарушения F6 SLA в течение срока оказания Услуг (срока действия Сертификата) способом, утвержденным Сторонами в Общих условиях оказания Услуг по Сертификатам или любого иного документа, по условиям которого Услуги оказываются (Сертификат реализуется) F6 и в котором содержится ссылка на Специальные условия.

4.5. Условия настоящего раздела о компенсации являются единственной и исчерпывающей мерой ответственности F6 за нарушение SLA.

5 ПРОЧИЕ УСЛОВИЯ

5.1. Специальные условия являются неотъемлемой частью Общих условий оказания Услуг по сертификатам или любого иного документа, по условиям которого Услуги оказываются F6 и в котором содержится ссылка на Специальные условия.

5.2. Специальные условия не являются офертой или публичной офертой по смыслу ст. 435, п. 2 ст. 437 ГК РФ, а именно: Специальные условия не содержат все существенные условия договора, не являются предложением заключить договор на указанных условиях с любым, кто на них отзовется. Во избежание сомнений Специальные условия вступают в силу и становятся обязательными для Сторон в порядке, установленном для документов, указанных в п. 4.1. Специальных условий.

5.3. F6 вправе вносить изменения в Специальные условия, при условии направления Заказчику соответствующего уведомления не менее чем за 30 (Тридцать) календарных дней до даты вступления таких изменений в силу. В этом случае F6, помимо направления уведомления, размещает новую редакцию Специальных условий по ссылке: https://www.f6.ru/law/services/SOC/special-terms.

Изменения вступают в силу на 31 (Тридцать первый) календарный день с даты направления со стороны F6 в адрес Заказчика уведомления, если в самом уведомлении не указан иной срок вступления изменений в силу (в любом случае такой срок не может составлять менее 30 (Тридцати) календарных дней с даты направления уведомления).

5.4. Специальные условия регулируются в соответствии с законодательством Российской Федерации.

5.5. Действующая версия Специальных условий размещена в сети Интернет по постоянному адресу: https://www.f6.ru/law/services/SOC/special-terms.