F6

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

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

Специальные условия оказания услуг «Ретейнер F6»

Действующая версия № 1.0 от «25» декабря 2025 г.

Оглавление

1. Сокращения

- **ВПО** – вредоносное программное обеспечение.
- **ИБ** – информационная безопасность.
- **ИС** – информационная система.
- **ИСПДн** – информационная система персональных данных.
- **КИИ** – критическая информационная инфраструктура.
- **КТ** – коммерческая тайна.
- **ЛВС** – локальная вычислительная сеть.
- **ОРД** – организационно-распорядительная документация.
- **ОС** – операционная система.
- **ПДн** – персональные данные.
- **ПО** – программное обеспечение.
- **СЗИ** – средства защиты информации.
- **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).

2. Описание, ограничения и сроки оказания услуг

Аудит информационной безопасности[1]	
Услуга: внешнее тестирование (формат «Тестирование на проникновение»)	
Описание услуги	Услуга направлена на поиск недостатков и уязвимостей внешней сетевой инфраструктуры, доступной из сети Интернет. Основной акцент делается на «глубину» анализа и достижение определенных целей, выстраивание килчейна атак. Особое внимание уделяется уязвимостям, цепочка эксплуатации которых позволяет достичь определенного результата (например, преодоление внешнего периметра) и продемонстрировать векторы атак.

[1] Соглашаясь с оказанием услуг, входящих в аудит информационной безопасности, Заказчик понимает, что производимые действия, если бы они не были санкционированы Заказчиком, потенциально могли бы квалифицироваться в соответствии с положениями статей главы 28 действующего Уголовного кодекса Российской Федерации, и признает, что услуги оказываются с его согласия, и он не будет иметь претензий к Исполнителю в отношении любых действий, проводимых Исполнителем в рамках оказания таких услуг.

Состав услуги[2]

В рамках услуги Исполнитель может совершать следующие действия[3]**:**

1. Проведение внешней сетевой разведки:

- Сбор информации о внешней сетевой инфраструктуре Заказчика, доступной из сети Интернет;
- Составление списка узлов внешнего сетевого периметра (IP-адресов сетевых устройств, доменных имен и сервисов внешней сетевой инфраструктуры), принадлежащих Заказчику;
- Фиксация ограничений и целей, согласование с Заказчиком по электронной почте перечня обнаруженных узлов внешнего сетевого периметра.

Результаты оказания услуги по данному этапу:

- Собрана и проанализирована информация из публично доступных источников сети Интернет;
- Заказчиком согласована область оказания услуги и ограничения по перечню действий F6 в рамках оказания услуги.

2. Выявление уязвимостей и построение релевантных векторов атак:

- Определение внешних сетевых узлов, относящихся к ключевым информационным системам Заказчика;
- Поиск уязвимостей, которые могут быть использованы для преодоления внешнего сетевого периметра;
- Построение потенциальных векторов атак, направленных на получение несанкционированного доступа к сетевой инфраструктуре Заказчика.

Результаты оказания услуги по данному этапу:

- Сформирован перечень уязвимостей, которые могут быть использованы для преодоления внешнего сетевого периметра Заказчика;
- Определены векторы атак на внешние системы Заказчика (согласованы потенциально деструктивные векторы атак с Заказчиком).

3. Верификация доступных векторов атак:

- Верификация и апробация полученных векторов атак в ручном и полу-автоматизированном режиме;
- Анализ первичных результатов, определение дальнейших методов продвижения с целью получения доступа к ключевым сетевым активам Заказчика.

[2] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[3] Оказание 2-5 этапов услуги возможно только после согласования Заказчиком области оказания услуги и ограничений по перечню действий F6 по результатам 1 этапа оказания услуги.

Результаты оказания услуги по данному этапу:

- Векторы атак сформированы в цепочки/последовательности, отражающие возможные действия потенциального злоумышленника;
- Векторы атак проверены, определены работоспособные, получен первичный доступ в системы Заказчика и подтверждена возможность развития атаки вглубь.

4. Моделирование атак в отношении систем:

Демонстрация эксплуатации уязвимостей и работоспособности векторов атак, моделирование действий потенциальных злоумышленников по получению доступа к узлам внешнего сетевого периметра, относящимся к ключевым информационным системам Заказчика.

Результаты оказания услуги по данному этапу:

Собраны подтверждения работоспособности и эффективности цепочек/последовательностей атак.

5. Подготовка отчетной документации:

- Описание перечня проведенных проверок по поиску уязвимостей;
- Описание методов и способов эксплуатации выявленных уязвимостей и векторов атак;
- Разработка рекомендаций по устранению выявленных уязвимостей и недостатков ИБ.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, применительно к внешним информационным системам Заказчика, а также рекомендации по повышению уровня защищенности и выводы для технических специалистов и руководства Заказчика.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что:

- Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей информационных систем Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности сервисов Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов;
- Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности этих информационных систем. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с

	текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании информационных систем Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 23 рабочих дня. • Минимальное количество часов, необходимое для оказания услуги - 90 часов. • Срок начала оказания услуги - до 20 рабочих дней.

Услуга: внешнее тестирование (формат «Анализ защищенности»)

Описание услуги	Услуга направлена на поиск недостатков и уязвимостей внешней сетевой инфраструктуры, доступной из сети Интернет. Основной акцент делается на «ширину» анализа - выявление максимального числа уязвимостей и недостатков вне зависимости от степени их потенциального воздействия (включает уязвимости, использование которых не несет непосредственных рисков либо эксплуатация которых в системах Заказчика крайне затруднена).
Состав услуги[4]	**В рамках услуги F6 может совершать следующие действия:**[5] **1. Проверка доступа:** • Проверка корректности созданных исключений на стороне СЗИ Заказчика; • Фиксация ограничений и целей по определенному перечню действий F6 в рамках оказания услуги. **Результаты оказания услуги по данному этапу:** Заказчиком согласована область оказания услуги и ограничения по перечню действий F6 в рамках оказания услуги. **2. Обследование внешней информационно-технологической инфраструктуры Заказчика:** • Изучение доступных узлов внешнего сетевого периметра (IP-адресов сетевых устройств, доменных имен и сервисов внешней сетевой инфраструктуры); • Сканирование узлов внешнего сетевого периметра, изучение по реакции на внешнее воздействие; • Сбор информации о доступных внешних сетевых службах и сервисах.

[4] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[5] В целях оказания услуги Заказчик обязуется до даты начала оказания услуги предоставить F6 список, содержащий IP-адреса, подсети, доменные имена и сервисы внешней сетевой инфраструктуры Заказчика, а также обеспечить доступ F6 к исследуемой инфраструктуре на сетевом уровне (в том числе, внести IP-адреса F6 в белые списки СЗИ).

Результаты оказания услуги по данному этапу:

- Произведена систематизация и анализ данных о структуре и топологии внешней сети Заказчика;
- Сформирован перечень доступных узлов внешнего сетевого периметра Заказчика.

3. Выявление недостатков и уязвимостей внешних сетевых ресурсов, их верификация и эксплуатация:

- Поиск уязвимостей в ручном и автоматизированном режиме;
- Анализ первичных результатов, ручная верификация обнаруженных недостатков.

Результаты оказания услуги по данному этапу:

Проведена проверка недостатков ИБ на предмет возможности использования потенциальным злоумышленником при атаках на внешние информационные системы Заказчика.

4. Выявление недостатков конфигурации сети:

Проверка на наличие типовых архитектурных недостатков сети и особенностей систем, которые могут быть использованы злоумышленником для атак на информационные системы Заказчика.

Результаты оказания услуги по данному этапу:

Произведен анализ возможных недостатков конфигураций узлов внешнего сетевого периметра Заказчика.

5. Подготовка отчетной документации:

- Описание перечня проведенных проверок по поиску уязвимостей;
- Описание методов и способов эксплуатации выявленных уязвимостей;
- Разработка рекомендаций по устранению выявленных уязвимостей и недостатков ИБ.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию уязвимостей применительно к внешним информационным системам Заказчика, а также рекомендации по повышению уровня защищенности и выводы для технических специалистов и руководства Заказчика.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что:

- Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей информационных систем Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности

	сервисов Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов; • Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности этих информационных систем. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании информационных систем Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 23 рабочих дня. • Минимальное количество часов, необходимое для оказания услуги - 90 часов. • Срок начала оказания услуги - до 20 рабочих дней.
Услуга: внутреннее тестирование (формат «Тестирование на проникновение»)	
Описание услуги	Услуга направлена на поиск недостатков и уязвимостей во внутренней корпоративной сети. Основной акцент делается на «глубину» анализа, достижение определенных целей и выстраивание векторов атак. Особое внимание уделяется уязвимостям, цепочка эксплуатации которых позволяет достичь определенного результата (например, повышение привилегий в ЛВС) и продемонстрировать возможные атаки.
Состав услуги[6]	**В рамках услуги F6 может совершать следующие действия:[7]** **1. Проверка доступа:** • Организация доступа к ЛВС Заказчика; • Фиксация ограничений и целей по определенному перечню действий F6 в рамках оказания услуги. **Результаты оказания услуги по данному этапу:** F6 получен и проверен доступ к исследуемой ЛВС, с Заказчиком согласованы ограничения по перечню действий F6 в рамках оказания услуги. **2. Обследование информационно-технологической инфраструктуры Заказчика:** • Проведение внутренней сетевой разведки в ЛВС Заказчика;

[6] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[7] В качестве начальной точки оказания услуги Заказчик перед датой начала оказания услуг обязуется предоставить F6 типовой доступ к ЛВС Заказчика. Допускается установление Заказчиком входных ограничений на подключение F6 к исследуемой инфраструктуре. В таком случае преодоление указанных ограничений является неотъемлемой частью услуги (к возможным ограничениям относятся: блокировки СЗИ, отсутствие у F6 свободного доступа к ЛВС Заказчика, отсутствие у F6 возможности использовать специальные инструменты автоматизированной проверки).

- Поиск узлов ЛВС (серверов и сервисов ЛВС), относящихся к ключевым информационным системам.

Результаты оказания услуги по данному этапу:

Проанализирована область исследования, сформирована поверхность атаки.

3. Выявление и верификация уязвимостей систем, находящихся в ЛВС Заказчика:

- Поиск потенциальных векторов атак, направленных на получение несанкционированного доступа к ЛВС;
- Анализ первичных результатов, верификация и апробация полученных векторов атак в ручном и автоматизированном режиме.

Результаты оказания услуги по данному этапу:

- Проверены векторы атак, определены работоспособных, получен первичный доступ в ЛВС и подтверждена возможность развития атаки вглубь;
- Сформированы векторы атак в цепочки/последовательности, отражающие возможные действия потенциального злоумышленника.

4. Моделирование атак в отношении ЛВС Заказчика:

- Демонстрация эксплуатации уязвимостей и работоспособности векторов атак, моделирование действий потенциальных злоумышленников по получению доступа к ключевым информационным системам Заказчика.

Результаты оказания услуги по данному этапу:

- Собраны подтверждения работоспособности и эффективности цепочек/последовательностей атак.

5. Подготовка отчетной документации. Выработка рекомендаций:

- Описание перечня проведенных проверок по поиску уязвимостей;
- Описание методов и способов эксплуатации выявленных уязвимостей и векторов атак;
- Разработка рекомендаций по устранению выявленных уязвимостей и недостатков ИБ.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей применительно к ЛВС Заказчика, а также рекомендации по повышению уровня защищенности и выводы для технических специалистов и руководства Заказчика.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что:

- Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей

	информационных систем Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности сервисов Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов; • Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности этих информационных систем. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании информационных систем Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 25 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 100 часов. • Срок начала оказания услуги - до 30 рабочих дней.
Услуга: внутреннее тестирование (формат «Анализ защищенности»)	
Описание услуги	Услуга направлена на поиск недостатков и уязвимостей во внутренней корпоративной сети. Основной акцент делается на «ширину» анализа - выявление максимального числа уязвимостей и недостатков вне зависимости от степени их потенциального воздействия (включает уязвимости, использование которых не несет непосредственных рисков либо эксплуатация которых в системах Заказчика крайне затруднена).
Состав услуги[8]	**В рамках услуги F6 может совершать следующие действия:[9]** **1. Проверка доступа:** • Организация доступа к ЛВС Заказчика; • Фиксация ограничений и целей по определенному перечню действий F6 в рамках оказания услуги. **Результаты оказания услуги по данному этапу:** F6 получен и проверен доступ к исследуемой ЛВС, с Заказчиком согласованы ограничения по перечню действий F6 в рамках оказания услуги.

[8] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[9] В целях оказания услуги Заказчик обязуется до даты начала оказания услуги предоставить F6 прямой VPN-доступ к сети Заказчика или установить в ЛВС Заказчика рабочую станцию F6, обеспечить доступ F6 к исследуемой инфраструктуре на сетевом уровне (в том числе внести IP-адреса F6 в белые списки СЗИ), а также предоставить F6 список, содержащий узлы ЛВС Заказчика.

2. **Обследование информационно- технологической инфраструктуры Заказчика:**

- Сбор информации об инфраструктуре Заказчика, доступной из выделенного сегмента;
- Изучение доступных узлов ЛВС (серверов и сервисов ЛВС) и топологии доступных сетей.

Результаты оказания услуги по данному этапу:

- Определена топология сети (адресация и используемые наименования для узлов ЛВС);
- Топология соотнесена с областью оказания услуги, согласована с Заказчиком (при необходимости).

3. **Выявление уязвимостей и недостатков систем, находящихся в ЛВС Заказчика:**

- Сканирование доступных узлов ЛВС, изучение по реакции на оказываемое воздействие;
- Поиск уязвимостей в ручном и автоматизированном режиме, а также их ручная верификация.

Результаты оказания услуги по данному этапу:

Определен и сформирован верифицированный перечень уязвимостей и недостатков ИБ, которые может использовать потенциальный злоумышленник при атаке на узлы ЛВС Заказчика.

4. **Выявление недостатков конфигурации ЛВС Заказчика:**

Проверка на наличие типовых архитектурных недостатков и особенностей ЛВС, которые могут быть использованы злоумышленником для атак на ЛВС.

Результаты оказания услуги по данному этапу:

Проведена проверка архитектурных недостатков ЛВС Заказчика.

5. **Подготовка отчетной документации:**

- Описание перечня проведенных проверок по поиску уязвимостей;
- Описание методов и способов эксплуатации выявленных уязвимостей;
- Разработка рекомендаций по устранению выявленных уязвимостей и недостатков ИБ.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию уязвимостей применительно к ЛВС Заказчика, а также рекомендации по повышению уровня защищенности и выводы для технических специалистов и руководства Заказчика.

Требования и ограничения	**Заказчик проинформирован и согласен с тем, что:** • Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей информационных систем Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности сервисов Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов; • Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности этих информационных систем. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании информационных систем Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 25 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 100 часов. • Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование беспроводных (Wi-Fi) сетей

Описание услуги	Услуга направлена на оценку уровня защищенности точек доступа Wi-Fi, а также недостатков в архитектуре и организации беспроводного доступа.
Состав услуги[10]	**В рамках услуги F6 может совершать следующие действия:**[11] **1. Проведение сетевой разведки и сбор предварительной информации:** • Сбор предварительной информации о беспроводной сети Заказчика; • Анализ используемых схем и протоколов аутентификации и сегментации; • Поиск утечек данных о Wi-Fi в открытых источниках в сети Интернет.

[10] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[11] Заказчик обязуется не позднее, чем за 5 (Пять) рабочих дней до даты начала оказания услуги предоставить F6 перечень наименований точек доступа Wi-Fi сетей, входящих в область оказания услуги, данные учетных записей тестируемых Wi-Fi сетей и организовать специалистам F6 доступ на территорию покрытия указанных Wi-Fi сетей.

Результаты оказания услуги по данному этапу:

Определена область оказания услуги.

2. **Выявление уязвимостей и недостатков беспроводной сети Заказчика:**[12]

- Выявление потенциально слабых мест в схеме аутентификации;
- Проведение атак при схеме аутентификации по общему ключу (PSK);
- Проведение атак при аутентификации через централизованные RADIUS-серверы (Enterprise mode);
- Поиск явных недостатков в управлении доступом.

Результаты оказания услуги по данному этапу:

- Проведен анализ протоколов аутентификации;
- Выявлены потенциально «слабые места» в исследуемой инфраструктуре беспроводной сети Заказчика.

3. **Оценка возможности реализации угроз через беспроводную сеть Заказчика**[13]**:**

- Анализ конфигурации беспроводной сети на канальном уровне (OSI L2);
- Сканирование сегментов основной офисной сети;
- Анализ уязвимостей доступа к сетевым службам и сервисам.

Результаты оказания услуги по данному этапу:

Определена возможность или невозможность дальнейшего развития атаки в основной сегмент ЛВС Заказчика.

4. **Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:**

- Описание выявленных уязвимостей и векторов атак, а также методов эксплуатации;
- Разработка рекомендаций по устранению выявленных уязвимостей;
- Классификация уязвимостей, оценка уровня риска и критичности.

Результаты оказания услуги по данному этапу:

Совершены действия по моделированию угроз за счет эксплуатации найденных уязвимостей.

[12] Данный этап услуги оказывается на территории Заказчика.

[13] Данный этап услуги оказывается только в случае получения доступа к беспроводной сети Заказчика на предыдущих этапах оказания услуги. По согласованию с Заказчиком данный этап услуги может оказываться на территории Заказчика.

Требования и ограничения	Заказчик проинформирован и согласен с тем, что вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей беспроводных сетей Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности беспроводных сетей Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.
Срок оказания услуги	• Минимальный срок оказания услуги – 8 рабочих дней, при условии нахождения площадки тестирования в г. Москва. • Минимальное количество часов, необходимое для оказания услуги - 40 часов. • Срок начала оказания услуги - до 20 рабочих дней.

Услуга: социотехническое тестирование

Описание услуги	Услуга позволяет проверить текущий уровень осведомленности сотрудников Заказчика в вопросах обеспечения информационной безопасности.
Состав услуги[14]	**В рамках услуги F6 может совершать следующие действия:**[15] **1. Сбор информации:** • Поиск в сети Интернет публичных данных о Заказчике, выявление его ключевых особенностей; • Получение списка пользователей от Заказчика, включая целевые группы. **Результаты оказания услуги по данному этапу:** Собрана первичная информация. **2. Разработка инструментария тестирования:** • Разработка сценария и легенды для тестирования; • Согласование сценария, легенды и формата сбора данных с Заказчиком; • Разработка и согласование инструментария для тестирования (веб-сайты, исполняемые файлы и тексты сообщений). **Результаты оказания услуги по данному этапу:**

[14] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[15] Заказчик обязуется не позднее, чем за 5 (Пять) рабочих дней до даты начала оказания услуги предоставить F6 корпоративные почтовые адреса тестируемой фокус-группы и доступы к инфраструктуре, необходимые F6 для проведения тестирования в рамках согласованного сценария, а также настраивает свои системы и средства защиты информации для беспрепятственной доставки писем с IP-адресов F6, с которых будет оказываться услуга.

- Создан инструментарий для тестирования в соответствии с легендами;
- Согласован формат тестирования по каждой целевой группе.

3. Тестирование работоспособности инструментария:

- Создание исключений на средствах защиты информации Заказчика;
- Проверка инструментария проекта на выборочных получателях Заказчика.

Результаты оказания услуги по данному этапу:

- Совершены действия по взаимодействию со специалистами Заказчика;
- Средства защиты не блокируют рассылку.

4. Проведение социотехнического тестирования:

Реализация сценария тестирования.

Результаты оказания услуги по данному этапу:

Проведена имитация социотехнической атаки.

5. Документирование и анализ результатов:

- Обработка результатов;
- Разработка отчета и выработка рекомендаций.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий выводы об осведомленности целевой группы сотрудников Заказчика, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что:

- Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей информационных систем Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности сервисов Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.

Срок оказания услуги

- Минимальный срок оказания услуги – 10 рабочих дней.
- Минимальное количество часов, необходимое для оказания услуги - 50 часов.
- Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование веб-приложения без обращения к исходному коду (полная методика, объект – статичное приложение)

Описание услуги	Услуга направлена на выявление уязвимостей и недостатков в простых веб-приложениях, таких как лендинги, сайты-визитки и пр.
Состав услуги[16]	**В рамках услуги F6 может совершать следующие действия:**[17] **1. Выявление уязвимостей в окружении веб-приложения Заказчика:** Сбор информации и первичный анализ окружения приложения. **Результаты оказания услуги по данному этапу:** Выявлены потенциальные «слабые места» в окружении веб-приложения Заказчика. **2. Выявление уязвимостей в веб-приложении Заказчика:** Проведение ручного и автоматизированного тестирования основных функций приложения и его механизмов безопасности. **Результаты оказания услуги по данному этапу:** • Произведен ручной и автоматизированный поиск уязвимостей; • Сформирован перечень выявленных недостатков и уязвимостей. **3. Подтверждение возможности эксплуатации обнаруженных уязвимостей:** • Эксплуатация обнаруженных уязвимостей; • Определение угроз, реализуемых через выявленные уязвимости. **Результаты оказания услуги по данному этапу:** Совершены действия по моделированию угроз за счет эксплуатации найденных уязвимостей. **4. Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:** • Описание выявленных уязвимостей и векторов атак, а также методов эксплуатации; • Классификация уязвимостей, оценка уровня риска и критичности; • Разработка рекомендаций по устранению выявленных уязвимостей.

[16] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[17] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к тестовому стенду веб-приложения Заказчика, в отношении которого будет оказываться услуга. В случае отсутствия тестового стенда веб-приложения Заказчик обязуется предоставить F6 URL-адрес веб-приложения Заказчика, в отношении которого будет оказываться услуга. Для полноценного оказания услуги Заказчику необходимо внести IP-адреса F6 в белые списки WAF.

	Результаты оказания услуги по данному этапу: Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.
Требования и ограничения	**Заказчик проинформирован и согласен с тем, что:** • Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей веб-приложения Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности веб-приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов; • Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности веб-приложения. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании веб-приложения Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 12 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 60 часов. • Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование веб-приложения без обращения к исходному коду (полная методика, объект - приложение с функцией личных кабинетов/с функцией платежей/онлайн-банкинга)

Описание услуги	Услуга направлена на выявление уязвимостей и недостатков в веб-приложениях с функциональностью личных кабинетов или проведения платежей пользователями (например интернет-магазины), или интернет-банкинга.
Состав услуги[18]	**В рамках услуги F6 может совершать следующие действия:**[19]

[18] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[19] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к тестовому стенду веб-приложения Заказчика, в отношении которого будет оказываться услуга, а по согласованию Сторон - также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в веб-приложении. В случае отсутствия тестового стенда веб-приложения Заказчик обязуется предоставить F6 URL-адрес веб-приложения Заказчика, в отношении которого будет оказываться услуга, а по согласованию Сторон - также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в веб-приложении. Для полноценного оказания услуги Заказчику необходимо внести IP-адреса F6 в белые списки WAF. Для оказания услуги в отношении объекта с функцией платежей Заказчику также необходимо начислить виртуальные денежные средства на тестовые учетные записи F6.

1. **Сбор информации и первичный анализ:**

- Сбор первичной информации в открытых источниках сети Интернет;
- Идентификация элементов инфраструктуры веб-приложения и элементов информационного окружения;
- Определение структуры веб-приложения.

Результаты оказания услуги по данному этапу:

Собрана первичная информация о функциональных возможностях, построена карта веб-приложения Заказчика.

2. **Выявление уязвимостей в веб-приложении Заказчика:**

- Тестирование конфигурации и управления развертыванием;
- Тестирование аутентификации, механизма сессий, авторизации и идентификации;
- Тестирование валидации входных данных и обработки ошибок;
- Тестирование на предмет некриптостойкого шифрования;
- Тестирование механизмов безопасности клиентской части и ошибок бизнес-логики.

Результаты оказания услуги по данному этапу:

- Произведен ручной и автоматизированный поиск уязвимостей;
- Сформирован перечень выявленных недостатков веб-приложения Заказчика.

3. **Подтверждение возможности эксплуатации обнаруженных уязвимостей:**

- Эксплуатация обнаруженных уязвимостей;
- Определение угроз, реализуемых через выявленные уязвимости;
- Оценка возможности увеличения поверхности атаки.

Результаты оказания услуги по данному этапу:

Совершены действия по моделированию угроз за счет эксплуатации найденных уязвимостей.

4. **Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:**

- Описание выявленных уязвимостей и методов эксплуатации;
- Классификация и оценка уровня риска выявленных уязвимостей;
- Разработка рекомендаций по устранению выявленных уязвимостей.

Результаты оказания услуги по данному этапу:

	Подготовлен отчет, содержащий систематизацию выявленных уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.
Требования и ограничения	**Заказчик проинформирован и согласен с тем, что:** • Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей веб-приложения Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности веб-приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов; • Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности веб-приложения. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании веб-приложения Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 25 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 120 часов. • Срок начала оказания услуги - до 30 рабочих дней.
Услуга: тестирование веб-приложения без обращения к исходному коду (сокращенная методика)	
Описание услуги	Услуга направлена на выявление уязвимостей и недостатков в веб-приложениях на основании списка проверок OWASP Web Top 10 и опыта специалистов департамента F6 в направлении наиболее часто встречаемых недостатков.
Состав услуги[20]	**В рамках услуги F6 может совершать следующие действия:**[21] **1. Сбор информации и первичный анализ:** Идентификация элементов инфраструктуры веб-приложения и элементов информационного окружения Заказчика. **Результаты оказания услуги по данному этапу:**

[20] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[21] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к тестовому стенду веб-приложения Заказчика, в отношении которого будет оказываться услуга, а по согласованию Сторон - также тестовые учетные записи относительно каждой роли, предусмотренной в веб-приложении. Для полноценного оказания услуги Заказчику необходимо внести IP-адреса F6 в белые списки WAF.

Собрана первичная информация о функциональных возможностях.

2. **Выявление уязвимостей в веб-приложении Заказчика:**

- Тестирование конфигурации и управления развертыванием;
- Тестирование идентификации, аутентификации;
- Тестирование механизма сессий и авторизации;
- Тестирование ошибок валидации входных данных и обработки ошибок;
- Тестирование на предмет некриптостойкого шифрования.

Результаты оказания услуги по данному этапу:

- Произведен ручной и автоматизированный поиск уязвимостей в рамках перечня проверок OWASP Top-10;
- Сформирован перечень выявленных недостатков и уязвимостей.

3. **Подтверждение возможности эксплуатации обнаруженных уязвимостей:**

- Верификация обнаруженных уязвимостей;
- Определение угроз, реализуемых через выявленные уязвимости.

Результаты оказания услуги по данному этапу:

Совершены действия по верификации обнаруженных уязвимостей и моделированию угроз их эксплуатации.

4. **Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:**

- Описание выявленных уязвимостей и векторов атак, а также методов эксплуатации;
- Классификация уязвимостей, оценка уровня риска и критичности;
- Разработка рекомендаций по устранению выявленных уязвимостей.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что:

- Вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей веб-приложения Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности веб-приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов;

	• Для целей оказания услуги F6 необходимо проведение тестирования в формате фаззинга, которое в случае недостаточной конфигурации информационных систем Заказчика и связанных с ними инфраструктурных компонентов, может негативным образом отразиться на работоспособности и доступности веб-приложения. В рамках оказания услуги F6 обязуется ограничиваться только теми проверками, которые в соответствии с текущим уровнем знаний F6 об объекте тестирования, не могут привести к отказу в обслуживании веб-приложения Заказчика.
Срок оказания услуги	• Минимальный срок оказания услуги – 10 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 50 часов. • Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование мобильного приложения без обращения к исходному коду (сокращенная методика)

Описание услуги	Услуга направлена на выявление уязвимостей и недостатков в мобильных приложениях на основании списка проверок OWASP Mobile Top 10 и опыта специалистов департамента F6 в направлении наиболее часто встречаемых недостатков. Не включает тестирование API.
Состав услуги[22]	**В рамках услуги F6 может совершать следующие действия:**[23] **1. Анализ функциональных особенностей мобильного приложения Заказчика:** • Сбор информации и первичный анализ используемого стека технологий; • Исследование функциональных возможностей мобильного приложения. **Результаты оказания услуги по данному этапу:** Определен перечень используемых технологий и уточнена область исследования, построена карта мобильного приложения Заказчика. **2. Выявление уязвимостей в мобильном приложении Заказчика:** • Тестирование на предмет безопасного хранения данных; • Тестирование аутентификации и механизма сессий; • Тестирование безопасности передачи данных;

[22] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[23] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к тестовому стенду мобильного приложения, в отношении которого будет оказываться услуга, а также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в мобильном приложении. В случае отсутствия тестового стенда мобильного приложения Заказчик предоставляет F6 URL-адрес для загрузки (скачивания) дистрибутива мобильного приложения, в отношении которого будет оказываться услуга, а также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в мобильном приложении. Все действия по услуге совершаются в отношении указанной на этапе старта оказания услуги версии мобильного приложения.

	• Тестирование конфигурации сборки и небезопасных методов программирования, а также устойчивости к реверс-инжинирингу. **Результаты оказания услуги по данному этапу:** • Произведен ручной и автоматизированный поиск уязвимостей; • Сформирован перечень выявленных недостатков и уязвимостей. **3. Подтверждение возможности эксплуатации обнаруженных уязвимостей:** • Эксплуатация обнаруженных уязвимостей; • Определение угроз, реализуемых через выявленные уязвимости; • Построение потенциальных векторов атак, направленных на получение несанкционированного доступа. **Результаты оказания услуги по данному этапу:** Совершены действия по моделированию угроз за счет эксплуатации найденных уязвимостей **4. Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:** • Описание выявленных уязвимостей, а также методов эксплуатации; • Классификация уязвимостей, оценка уровня риска и критичности; • Разработка рекомендаций по устранению выявленных уязвимостей. **Результаты оказания услуги по данному этапу:** Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.
Требования и ограничения	Заказчик проинформирован и согласен с тем, что вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей мобильного приложения Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности мобильного приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.
Срок оказания услуги	• Минимальный срок оказания услуги – 12 рабочих дней на 1 мобильную платформу (iOS или Android). • Минимальное количество часов, необходимое для оказания услуги - 60 часов. • Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование мобильного приложения без обращения к исходному коду (полная методика)

Описание услуги	Услуга направлена на выявление уязвимостей и недостатков в мобильных приложениях на платформах iOS и Android (включая производные платформы, такие как Huawei). Включает тестирование API приложения.
Состав услуги[24]	**В рамках услуги F6 может совершать следующие действия:**[25] **1. Анализ функциональных особенностей мобильного приложения Заказчика:** • Сбор информации и первичный анализ используемого стека технологий; • Исследование функциональных возможностей приложения. **Результаты оказания услуги по данному этапу:** Определен перечень используемых технологий и уточнена область исследования, построена карта мобильного приложения Заказчика. **2. Выявление и анализ уязвимостей в мобильном приложении Заказчика:** • Тестирование на предмет безопасного хранения данных; • Тестирование на предмет некриптостойкого шифрования и анализ безопасности передачи данных; • Тестирование механизмов аутентификации и управления сессиями; • Тестирование взаимодействия с платформой; • Тестирование конфигурации сборки и небезопасных методов программирования, а также устойчивости к реверс-инжинирингу; • Определение возможных атак на бизнес-логику приложения. **Результаты оказания услуги по данному этапу:** • Произведен ручной и автоматизированный поиск уязвимостей в мобильном приложении Заказчика; • Сформирован перечень выявленных недостатков и уязвимостей.

[24] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[25] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к тестовому стенду мобильного приложения, в отношении которого будет оказываться услуга, а также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в мобильном приложении. В случае отсутствия тестового стенда мобильного приложения Заказчик предоставляет F6 URL-адрес для загрузки (скачивания) дистрибутива мобильного приложения, в отношении которого будет оказываться услуга, а также по 3 (Три) учетные записи относительно каждой роли, предусмотренной в мобильном приложении. Все действия по услуге совершаются в отношении указанной на этапе старта оказания услуги версии мобильного приложения.

3. **Выявление недостатков и уязвимостей в API мобильного приложения Заказчика:**

- Оценка на предмет раскрытия чувствительной информации и использования уязвимых программных компонентов;
- Тестирование механизмов аутентификации и управления сессиями;
- Тестирование механизмов авторизации и обработки ошибок.

Результаты оказания услуги по данному этапу:

Произведен ручной и автоматизированный поиск уязвимостей в используемых серверных компонентах. Сформирован перечень выявленных недостатков и уязвимостей API.

4. **Подтверждение возможности эксплуатации обнаруженных уязвимостей:**

- Эксплуатация обнаруженных уязвимостей;
- Определение угроз, реализуемых через выявленные уязвимости.

Результаты оказания услуги по данному этапу:

Совершены действия по моделированию угроз за счет эксплуатации найденных уязвимостей.

5. **Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:**

- Описание выявленных уязвимостей и векторов атак, а также методов эксплуатации;
- Классификация уязвимостей, оценка уровня риска и критичности;
- Разработка рекомендаций по устранению выявленных уязвимостей.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства.

Требования и ограничения

Заказчик проинформирован и согласен с тем, что вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей мобильного приложения Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности мобильного приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.

Срок оказания услуги

- Минимальный срок оказания услуги – 25 рабочих дней на 1 мобильную платформу (iOS или Android и его производных).

- Минимальный срок оказания услуги по тестированию Android-производных приложений (например, для платформы Huawei), в случае присутствия в объектах тестирования и Android-версии этого же приложения, составляет 25% от минимального срока тестирования его Android-версии.
- Минимальное количество часов, необходимое для оказания услуги: 120 часов на 1 мобильную платформу (iOS или Android и его производных).
- Срок начала оказания услуги - до 30 рабочих дней.

Услуга: тестирование смарт-контрактов

Описание услуги

Услуга направлена на выявление и попытки эксплуатации и ранжирование по степени воздействия уязвимостей, потенциально приводящих к хищению средств, нарушению логики работы контракта и прочим неблагоприятным последствиям для Заказчика.

Состав услуги[26]

В рамках услуги F6 может совершать следующие действия:[27]

1. Сбор и анализ информации:

- Фиксация версии смарт-контракта Заказчика;
- Изучение документации;
- Обзор архитектуры и среды использования;
- Изучение прочих данных, связанных с тестируемым контрактом Заказчика.

Результаты оказания услуги по данному этапу:

Вся информация об объекте исследования собрана и систематизирована.

2. Анализ исходного кода контракта Заказчика:

- Анализ используемых библиотек, архитектуры и зависимых контрактов;
- Обзорный анализ исходного кода;
- Ручной и инструментальный статический анализ исходного кода;
- Анализ синтаксических конструкций.

Результаты оказания услуги по данному этапу:

Произведен статический анализ кода и окружения. Осуществлен поиск уязвимостей и недостатков.

[26] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[27] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к исходному коду контракта, тестовой среде, документации и данным связанных с ним контрактов.

	3. Функциональное тестирование контракта Заказчика: • Динамический анализ исходного кода; • Поиск уязвимостей, логических ошибок и прочих недостатков контракта; • Моделирование векторов атак и их апробирование в рабочей среде контракта. **Результаты оказания услуги по данному этапу:** Произведено динамическое тестирование. Осуществлен поиск уязвимостей и недостатков. Смоделированы атаки. **4. Документирование и анализ результатов. Выработка рекомендаций по устранению уязвимостей:** • Описание выявленных уязвимостей и векторов атак, а также методов эксплуатации; • Классификация уязвимостей, оценка уровня риска и критичности; • Разработка рекомендаций по устранению выявленных уязвимостей. **Результаты оказания услуги по данному этапу:** Подготовлен отчет, содержащий систематизацию возможных атак и уязвимостей, а также рекомендации по повышению уровня защищенности и выводы для руководства Заказчика.
Требования и ограничения	Заказчик проинформирован и согласен с тем, что вследствие особенностей оказания услуги F6 не может быть гарантировано полное выявление всех уязвимостей смарт-контракта Заказчика. На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.
Срок оказания услуги	• Минимальный срок оказания услуги – 20 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги: 90 часов. • Срок начала оказания услуги - до 40 рабочих дней.
Услуга: проверка устранения выявленных в результате оказания услуги недостатков	
Описание услуги	Услуга оказывается после завершения услуги по внешнему тестированию и/или, внутреннему тестированию, и/или тестированию веб-приложения, и/или тестированию мобильного приложения, и/или тестированию смарт-контрактов. Услуга обеспечивает прозрачный и верифицированный процесс закрытия уязвимостей Заказчика, что важно для внутреннего контроля, отчётности, уполномоченных регуляторов и внешних аудиторов. Цель услуги — убедиться, что

	Заказчик корректно устранил обнаруженные ранее уязвимости, ошибки конфигурации и прочие недостатки, зафиксированные в итоговом отчёте первичного тестирования, а также подтвердить отсутствие появления побочных проблем.
Состав услуги[28]	**В рамках услуги F6 может совершать следующие действия:**[29] **1. Сбор и анализ информации:** • Получение от Заказчика перечня уязвимостей, заявленных как устранённые; • Фиксация ограничений и целей по определенному перечню действий F6 в рамках оказания услуги. **Результаты оказания услуги по данному этапу:** F6 получен и проверен доступ к объекту первичного исследования, с Заказчиком согласованы ограничения по перечню действий F6 в рамках оказания услуги. Получена информация по проведенным действиям Заказчика, направленным на исправление недостатков из перечня, указанного в первичном отчете о действиях, предоставленного в рамках основной услуги. **2. Проведение оценки корректности устранения ранее обнаруженных уязвимостей и недостатков ИБ:** • Анализ первичного отчёта и уточнение методик воспроизведения уязвимостей; • Проверка достижимости целей ретеста с учётом изменений, внесённых Заказчиком; • Повторная попытка эксплуатации выявленных уязвимостей выбранными ранее методами; • Проверка корректности реализации рекомендаций (конфигурационных, организационных, кодовых); • Фиксация фактических результатов: устранено / частично устранено / не устранено. **Результаты оказания услуги по данному этапу:** • Произведена верификация исправлений уязвимостей по перечню первичного отчета; • Сформирован перечень устраненных недостатков и уязвимостей. **Документирование и анализ результатов:** • Формирование итогового документа с указанием статуса каждой уязвимости: устранена / частично устранена / не устранена; • Детальная фиксация повторных доказательств (по аналогии с первичным отчётом, но ограниченно зоной ретеста);

[28] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[29] Заказчик обязуется до даты начала оказания услуги предоставить F6 доступ к объекту первоначального исследования, идентичный тому, что был использован ранее и описан в первичном отчете.

	• Рекомендации по улучшению безопасности при частичном или неуспешном устранении. **Результаты оказания услуги по данному этапу:** Подготовлено заключение, содержащее систематизацию по результатам оценки корректности устранение первично выявленных уязвимостей и недостатков ИБ.
Требования и ограничения	Заказчик проинформирован и согласен с тем, что вследствие особенностей оказания услуги F6 не может быть гарантирована оценка корректности исправления всех уязвимостей тестируемого объекта Заказчика из перечня первичного отчета (например, отсутствие возможности доступа к компоненту системы в результате изменений, внесённых Заказчиком при исправлении). На результат оказания услуги существенно влияет совокупность не зависящих от F6 факторов, в том числе эффективность работы активных средств защиты информации Заказчика, временные рамки работоспособности мобильного приложения Заказчика, периодичность обновления сервисов Заказчика, емкость интернет-каналов, стабильность работы сервисов интернет-провайдеров, хостинговых сервисов.
Срок оказания услуги	• Минимальный срок оказания услуги – 6 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 25 часов. • Срок начала оказания услуги - до 15 рабочих дней.
Услуга: оценка соответствия требованиям законодательства Российской Федерации о персональных данных	
Описание услуги	Услуга направлена на проверку соблюдения организацией норм и требований законодательства Российской Федерации в области обработки и защиты ПДн, разработку рекомендаций и необходимых ОРД.
Состав услуги[30]	**В рамках услуги F6 может совершать следующие действия:** **1. Обследование:** • Сбор информации о процессах обработки ПДн и ИСПДн Заказчика; • Подготовка модуля отчета, содержащего описание процессов обработки ПДн и структурно-функциональные характеристики ИСПДн Заказчика. **Результаты оказания услуги по данному этапу:** • Подготовлены свидетельства для совершения дальнейших действий;

[30] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

- Подготовлен модуль отчета, содержащий информацию об обследовании инфраструктуры Заказчика и процессов в области анализа.

2. Оценка соответствия:

- Оценка соответствия выполнения Заказчиком организационно-правовых требований Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ, Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Оценка соответствия реализации Заказчиком мер защиты информации и процессов обеспечения ИБ в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Результаты оказания услуги по данному этапу:

Подготовлен модуль отчета, содержащий результаты оценки выполнения организационно-правовых требований Заказчиком, а также рекомендации по приведению в соответствие.

3. Моделирование угроз ИБ:

- Разработка модели(-ей) угроз безопасности информации ИСПДн в соответствии с "Методический документ. Методика оценки угроз безопасности информации" ФСТЭК России от 05.02.2021.

Результаты оказания услуги по данному этапу:

Подготовлена(-ы) модель (модели) угроз безопасности информации.

4. Разработка (доработка) комплекта ОРД:

Разработка (доработка) комплекта ОРД в соответствии с требованиями законодательства Российской Федерации в области защиты ПДн.

Результаты оказания услуги по данному этапу:

Подготовлен комплект ОРД.

5. Разработка технического задания на создание системы защиты информации:

Разработка технического задания на создание системы защиты информации в соответствии с требованиями ГОСТ 34.602-2020.

Результаты оказания услуги по данному этапу:

- Подготовлено техническое задание на создание системы защиты информации.

Срок оказания услуги

Минимальный срок оказания услуги (5 ИСПДн, 1 юридическое лицо):

- По этапам 1 (обследование) и 2 (оценка соответствия) услуги - 33 рабочих дня;
- По этапам 1 (обследование), 2 (оценка соответствия), 3 (моделирование угроз ИБ) и 4 услуги (разработка (доработка) комплекта ОРД) - 51 рабочий день.

Минимальное количество часов, необходимое для оказания услуги (5 ИСПДн, 1 юридическое лицо):

- По этапам 1 (обследование) и 2 (оценка соответствия) услуги - 100 часов;
- По этапам 1 (обследование), 2 (оценка соответствия), 3 (моделирование угроз ИБ) и 4 услуги (разработка (доработка) комплекта ОРД) - 150 часов.
- Срок начала оказания услуги - до 20 рабочих дней.

Услуга: оценка соответствия требованиям ГОСТ Р 57580.1–2017

Описание услуги

Услуга направлена на проверку соблюдения Заказчиком требований, установленных стандартом относительно защиты информации в финансовых организациях.

Состав услуги[31]

В рамках услуги F6 может совершать следующие действия:

1. Обследование:

- Анализ исходных данных и внутренней документации Заказчика в сфере защиты информации. Уточнение области оценки и разработка плана обследования;
- Проведение интервью с работниками Заказчика в соответствии с установленным планом и сбор свидетельств аудита;
- Анализ собранных свидетельств аудита и оценка соответствия принятых мер защиты требованиям ГОСТ 57580.1–2017.

Результаты оказания услуги по данному этапу:

- Подготовлен план проведения аудита;
- Подготовлены свидетельства аудита и выводы по результатам оказания данного этапа услуги требованиям ГОСТ 57580.1–2017.

[31] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

2. **Моделирование угроз ИБ:**

   Разработка модели(ей) угроз безопасности информации.

   Результаты оказания услуги по данному этапу:

   Подготовлен(ы) модель(-и) угроз безопасности.

3. **Разработка отчетных документов:**

   Подготовка отчета о выполнении требований ГОСТ 57580.1–2017, а также разработка рекомендаций по устранению выявленных несоответствий.

   Результаты оказания услуги по данному этапу:

   Подготовлен отчет по результатам оказания данного этапа услуги, включающий рекомендации по устранению несоответствий.

4. **Разработка (доработка) комплекта ОРД:**

   Разработка (доработка) проектов внутренних документов в сфере защиты информации.

   Результаты оказания услуги по данному этапу:

   Подготовлены проекты внутренних документов в сфере защиты информации.

5. **Оценка корректности выполнения рекомендаций. Разработка финального заключения:**

- Анализ корректности выполнения выданных рекомендаций;
- Подготовка отчетов о выполнении требований ГОСТ Р 57580.1–2017.

Результаты оказания услуги по данному этапу:

Подготовлен отчет по результатам оказания данного этапа услуги.

Срок оказания услуги

Минимальный срок оказания услуги (1 контур, 1 отчет):

- По этапам 1 (обследование) и 3 (разработка отчетных документов) услуги - 32 рабочих дня.
- По этапам 1 (обследование), 3 (разработка отчетных документов), 4 (разработка (доработка) комплекта ОРД) и 5 (оценка корректности выполнения рекомендаций. Разработка финального заключения) услуги - 54 рабочих дня.

Минимальное количество часов, необходимое для оказания услуги (1 контур, 1 отчет):

- По этапам 1 (обследование) и 3 (разработка отчетных документов) услуги - 90 часов.
- По этапам 1 (обследование), 3 (разработка отчетных документов), 4 (разработка (доработка) комплекта ОРД) и 5 (оценка корректности выполнения рекомендаций. Разработка финального заключения) услуги - 160 часов.

- Срок начала оказания услуги - до 20 рабочих дней.

Услуга: оценка соответствия требованиям Положения Банка России № 851-П / 757-П / 821-П / 802-П

Описание услуги

Услуга направлена на проверку соблюдения требований, выдвигаемых соответствующими положениями Банка России, которые регламентируют защиту информации.

Состав услуги[32]

В рамках услуги F6 может совершать следующие действия:

1. Обследование:

- Анализ исходных данных и внутренней документации Заказчика в сфере защиты информации;
- Уточнение области оценки и разработка плана обследования;
- Проведение интервью с работниками Заказчика в соответствии с установленным планом и сбор свидетельств аудита;
- Оценка соответствия принятых мер защиты требованиям Положения № 851-П / 757-П / 821-П / 802-П.

Результаты оказания услуги по данному этапу:

- Подготовлен план проведения аудита;
- Подготовлены свидетельства аудита и выводы по результатам оценки соответствия требованиям Положения № 851-П / 757-П / 821-П / 802-П.

2. Разработка отчетных документов:

- Подготовка отчета о выполнении требований Положения № 851-П / 757-П / 821-П / 802-П;
- Разработка рекомендаций по устранению выявленных несоответствий;

Результаты оказания услуги по данному этапу:

Подготовлен отчет по результатам оценки соответствия, включающий рекомендации по устранению несоответствий.

3. Разработка комплекта ОРД:

Разработка комплекта ОРД (Разработка (доработка) проектов внутренних документов в сфере защиты информации)

Результаты оказания услуги по данному этапу:

Подготовлены проекты внутренних документов в сфере защиты информации.

[32] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

Срок оказания услуги	**Минимальный срок оказания услуги (в отношении одного положения Банка России):** • По этапам 1 (обследование) и 2 (разработка отчетных документов) услуги - 24 рабочих дня. • По этапам 1 (обследование), 2 (разработка отчетных документов) и 3 (разработка комплекта ОРД) услуги - 34 рабочих дня. **Минимальное количество часов, необходимое для оказания услуги (в отношении одного положения Банка России):** • По этапам 1 (обследование) и 2 (разработка отчетных документов) услуги - 80 часов. • По этапам 1 (обследование), 2 (разработка отчетных документов) и 3 (разработка комплекта ОРД) услуги - 100 часов. • Срок начала оказания услуги - до 20 рабочих дней.

Услуга: оценка соответствия лучшим практикам в области ИБ

Описание услуги	Услуга направлена на проверку соответствия Заказчика международным стандартам в области защиты данных.
Состав услуги[33]	**В рамках услуги F6 может совершать следующие действия:** **1. Обследование:** • Анализ организационно-распорядительной, нормативной и сопутствующей документации Заказчика; • Сбор сведений об ИС в границах проекта; • Подготовка отчета, содержащего описание текущей информационной инфраструктуры и ИС. **Результаты оказания услуги по данному этапу:** • Подготовлены свидетельства для совершения дальнейших действий; • Подготовлен модуль отчета, содержащий информацию об ИС и инфраструктуре в границах аудита. **2. Оценка соответствия системы менеджмента информационной безопасности (СМИБ):** • Сбор и анализ свидетельств аудита для оценки зрелости процессов СМИБ; • Оценка соответствия текущей СМИБ требованиям стандарта; **Результаты оказания услуги по данному этапу:**

[33] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

Подготовлен модуль отчета, содержащий результаты оценки соответствия СМИБ требованиям стандарта, а также рекомендации по устранению несоответствий.

3. **Оценка соответствия (меры ИБ):**

- Сбор и анализ свидетельств аудита для оценки зрелости реализованных мер ИБ;
- Оценка соответствия принятых мер ИБ требованиям стандарта.

Результаты оказания услуги по данному этапу:

Подготовлен модуль отчета, содержащий результаты оценки соответствия принятых мер ИБ требованиям стандарта, а также рекомендации по устранению несоответствий.

4. **Оценка рисков ИБ:**

Выбор подхода, разработка методики оценки рисков и вычисление итоговых значений рисков.

Результаты оказания услуги по данному этапу:

Разработаны ключевые риски ИБ, рекомендации по снижению данных рисков.

5. **Разработка дорожной карты развития ИБ:**

- Разработка целевого (to-be) состояния системы ИБ в контексте процессов, технологий и сотрудников;
- Разработка плана (roadmap) по достижению целевого состояния.

Результаты оказания услуги по данному этапу:

Подготовлена дорожная карта развития ИБ.

6. **Разработка (доработка) комплекта ОРД:**

Разработка (доработка) проектов внутренних документов в сфере защиты информации.

Результаты оказания услуги по данному этапу:

Подготовлены проекты внутренних документов в сфере защиты информации (до уровня частных политик).

7. **Помощь в подготовке к сертификационному аудиту по ISO 27001:**

Разработка проектов документов, необходимых для выполнения требований основного текста стандарта ISO 27001.

Результаты оказания услуги по данному этапу:

Подготовлены проекты документов.

Срок оказания услуги	**Минимальный срок оказания услуги (5 ИС):** • По этапам 1 (обследование) и 3 (оценка соответствия (меры ИБ)) услуги - 35 рабочих дней. • По этапам 1 (обследование) и 4 (оценка рисков ИБ) услуги - 33 рабочих дня. • По этапам 1 (обследование), 2 (оценка соответствия (СМИБ)), 3 (оценка соответствия (меры ИБ), 4 (оценка рисков ИБ) и 5 (разработка дорожной карты развития ИБ) услуги - 78 рабочих дней. **Минимальное количество часов, необходимое для оказания услуги (5 ИС):** • По этапам 1 (обследование) и 3 (оценка соответствия (меры ИБ)) услуги - 100 часов. • По этапам 1 (обследование) и 4 (оценка рисков ИБ) услуги - 90 часов. • По этапам 1 (обследование), 2 (оценка соответствия (СМИБ)), 3 (оценка соответствия (меры ИБ), 4 (оценка рисков ИБ) и 5 (разработка дорожной карты развития ИБ) услуги - 230 часов. • Срок начала оказания услуги - до 30 рабочих дней.
Услуга: услуги в сфере обеспечения безопасности КИИ	
Описание услуги	Услуга направлена на категорирование объектов КИИ, проверку соблюдения Заказчиком требований законодательства в области КИИ, разработку недостающих ОРД, а также подготовку рекомендаций в области защиты информации.
Состав услуги[34]	**В рамках услуги F6 может совершать следующие действия:** **1. Категорирование:** • Определение состава комиссии по категорированию объектов КИИ Заказчика; • Сбор информации о процессах, деятельности Заказчика для выявления перечня критических процессов; • Определение перечня объектов КИИ Заказчика, которые обрабатывают информацию, связанную с критическими процессами; • Определение угроз информационной безопасности объектов КИИ Заказчика, подлежащих категорированию; • Проведение категорирования объектов КИИ Заказчика (совместно с комиссией по категорированию); • Разработка отчетных документов для отправки во ФСТЭК России. **Результаты оказания услуги по данному этапу:**

[34] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

- Подготовлен приказ о создании комиссии;
- Подготовлено положение о комиссии;
- Подготовлен акт критических процессов;
- Подготовлен перечень объектов КИИ Заказчика;
- Подготовлен проект акта категорирования объектов КИИ Заказчика;
- Подготовлены сведения о результатах категорирования по форме Приказа ФСТЭК России №236;
- Подготовлена инструкция по отправке отчетных документов во ФСТЭК России.

2. Обследование:[35]

- Осуществляется сбор информации для совершения дальнейших действий;
- Разработка модуля отчета об обследовании, содержащего описание структурно-функциональных характеристик объектов КИИ.

Результаты оказания услуги по данному этапу:

- Подготовлены свидетельства для проведения дальнейших работ;
- Подготовлен модуль отчета об обследовании, содержащий описание структурно-функциональных характеристик объектов КИИ.

3. Оценка соответствия:

- Оценка соответствия процессов, систем, средств защиты информации требованиям Приказов ФСТЭК России №235 и №239;
- Оценка соответствия реализации мер защиты информации и процессов обеспечения ИБ требованиям Приказа ФСТЭК России №239;
- Оценка реализации требований к организационно-штатной структуре, ответственным лицам и средствам защиты информации в соответствии с Указом Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации";
- Оценка процесса информирования федерального органа исполнительной власти о компьютерных инцидентах.

Результаты оказания услуги по данному этапу:

- Подготовлен модуль отчета, содержащий результаты оценки выполнения организационно-правовых требований;

[35] Данный этап услуги проводится при условии, что Заказчик провел категорирование объектов КИИ своими силами или с привлечением третьих лиц. В случае проведения Исполнителем категорирования в рамках 1 этапа услуги, обследование в рамках 2 этапа услуги не проводится.

- Подготовлен модуль отчета, содержащий результаты оценки соответствия системы защиты требованиям, определенным Приказом ФСТЭК России №239;
- Подготовлен модуль отчета, содержащий результаты оценки соответствия Указу Президента №250;
- Подготовлен модуль отчета, содержащий результаты оценки соответствия процесса информирования федерального органа исполнительной власти о компьютерных инцидентах.

4. **Моделирование угроз ИБ:**

   Разработка модели(ей) угроз безопасности информации объектов КИИ в соответствии с "Методический документ. Методика оценки угроз безопасности информации" ФСТЭК России от 05.02.2021.

   Результаты оказания услуги по данному этапу:

   Подготовлен(ы) модель(-и) угроз безопасности информации.

5. **Разработка комплекта ОРД:**

   Разработка (доработка) комплекта ОРД в соответствии с требованиями законодательства РФ в области защиты КИИ.

   Результаты оказания услуги по данному этапу:

   Подготовлен комплект ОРД.

6. **Разработка технического задания на создание системы защиты информации:**

   Разработка технического задания на создание системы защиты информации в соответствии с требованиями ГОСТ 34.602 2020.

   Результаты оказания услуги по данному этапу:

   Подготовлено иехническое задание на создание системы защиты информации.

7. **Разработка верхнеуровневой дорожной карты создания/развития системы защиты информации:**

   Разработка дорожной карты (Разработка дорожной карты с учетом актуальных требований законодательства в области защиты КИИ к созданию и развитию системы защиты информации).

   Результаты оказания услуги по данному этапу:

   Подготовлена дорожная карта создания/развития системы защиты информации.

Срок оказания услуги	**Минимальный срок оказания услуги (3 объекта КИИ, 1 юридическое лицо):** • По этапу 1 (категорирование) услуги - 12 рабочих дней. • По этапу 2 (обследование) услуги - 7 рабочих дней.

- По этапам 1 (категорирование), 3 (оценка соответствия), 4 (моделирование угроз ИБ) и 5 (разработка комплекта ОРД) услуги - 48 рабочих дней.

Минимальное количество часов, необходимое для оказания услуги (3 объекта КИИ, 1 юридическое лицо):1) По этапу 1 (категорирование) услуги - 87 часов.

- По этапу 2 (обследование) услуги - 20 часов.
- По этапам 1 (категорирование), 3 (оценка соответствия), 4 (моделирование угроз ИБ) и 5 (разработка комплекта ОРД) услуги - 150 часов.
- Срок начала оказания услуги - до 20 рабочих дней.

Услуга: анализ мер защиты коммерческой тайны

Описание услуги

Услуга направлена на выявление потенциальных нарушений режима КТ путем анализа соответствия режима КТ требованиям законодательства Российской Федерации, разработку и/или доработку внутренних ОРД в области КТ.

Состав услуги[36]

В рамках услуги F6 может совершать следующие действия:

1. Обследование:

- Анализ действующей организационно-распорядительной, нормативной и сопутствующей документации Заказчика в области КТ;
- Подготовка отчета, содержащего описание ИС и обрабатываемой конфиденциальной информации в ней.

Результаты оказания услуги по данному этапу:

- Подготовлены свидетельства для проведения дальнейших работ.
- Подготовлен отчет, включающий перечень информации, составляющей КТ.

2. Оценка соответствия:

- Проведение интервью со структурными подразделениями Заказчика, сбор свидетельств установления режима коммерческой тайны в соответствии с требованиями ФЗ-98 «О коммерческой тайне»;
- Анализ собранных свидетельств аудита и выявление недостатков текущей системы защиты для введения юридически значимого режима КТ.

Результаты оказания услуги по данному этапу:

[36] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

	Подготовлен модуль отчета, включающий выводы о достаточности существующих мер защиты и рекомендации по введению режима КТ. **3. Разработка комплекта ОРД:** Разработка комплекта ОРД в соответствии с требованиями законодательства РФ в области защиты КТ **Результаты оказания услуги по данному этапу:** Подготовлен комплект ОРД.
Срок оказания услуги	**Минимальный срок оказания услуги (5 ИС в границах услуги, 1 юридическое лицо):** • По этапам 1 (обследование) и 2 (оценка соответствия) услуги - 18 рабочих дней. • По этапам 1 (обследование), 2 (оценка соответствия) и 3 (разработка комплекта ОРД) услуги - 23 рабочих дня. **Минимальное количество часов, необходимое для оказания услуги (5 ИС в границах услуги, 1 юридическое лицо):** • По этапам 1 (обследование) и 2 (оценка соответствия) услуги - 50 часов. • По этапам 1 (обследование), 2 (оценка соответствия) и 3 (разработка комплекта ОРД) услуги - 70 часов. • Срок начала оказания услуги - до 20 рабочих дней.
Услуга: единоразовые консультации в области ИБ/исполнения требований законодательства в области ИБ (в сфере КИИ, ПДн, КТ)	
Описание услуги	Услуга направлена на помощь Заказчику по возникающим у него вопросам, связанным с ИБ, исполнением требований законодательства в области ИБ и обработкой ПДн.
Состав услуги[37]	**В рамках услуги F6 может совершать следующие действия:** **1. Консультация в формате «Вопросы – ответы/рекомендации».** **Результаты оказания услуги по данному этапу:** Подготовлен документ с ответами/рекомендациями по каким-либо вопросам, связанным с ИБ/ требованиями законодательства в области ИБ. **Мини-проект:** Проведение мини-проекта в рамках малых границ аудита (например: не более 1-2 ИС и по 1-2 требованиям/доменам ИБ).

[37] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

Результаты оказания услуги по данному этапу:

Подготовлен модуль отчета, содержащий результаты оценки выполнения выбранных требований.

Срок оказания услуги

Минимальный срок оказания услуги:

- По 1 этапу (консультация в формате «Вопросы – ответы/рекомендации») услуги - 1 рабочий день.
- По 2 этапу (мини-проект) услуги - 3 рабочих дня.

Минимальное количество часов, необходимое для оказания услуги:

- По 1 этапу (консультация в формате «Вопросы – ответы/рекомендации») услуги - 8 часов.
- По 2 этапу (мини-проект) услуги - 16 часов.
- Срок начала оказания услуги - до 5 рабочих дней.

Цифровая криминалистика и исследование вредоносного кода[38]

Услуга: выявление следов компрометации

Описание услуги

Услуга направлена на комплексную проверку всей ИТ-инфраструктуры с целью обнаружения признаков несанкционированного доступа, нелегитимной активности и скрытых угроз, которые могут оставаться незамеченными, в том числе для средств защиты информации, длительное время. Обнаружение угроз позволяет локализовать их, лишить злоумышленников возможности взаимодействия со скомпрометированными системами и установить причины их возникновения при достаточном количестве цифровых следов.

Состав услуги[39]

В рамках услуги F6 может совершать следующие действия:[40]

1. **Определение источников цифровых следов.**

   На основе информации, предоставленной Заказчиком в опросном листе, специалистами F6 определяется перечень источников цифровых следов. В данный перечень могут входить различные источники цифровых следов, например журналы событий ОС, различных прикладных программ и сервисов, файлы системных и пользовательских реестров ОС Windows, файлы конфигураций

[38] Соглашаясь с оказанием услуг, входящих в цифровую криминалистику и исследование вредоносного кода, Заказчик понимает, что производимые действия, если бы они не были санкционированы Заказчиком, потенциально могли бы квалифицироваться в соответствии с положениями статей главы 28 действующего Уголовного кодекса Российской Федерации, и признает, что услуги оказываются с его согласия, и он не будет иметь претензий к Исполнителю в отношении любых действий, проводимых Исполнителем в рамках оказания таких услуг.

[39] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

[40] Заказчик обязуется до даты начала оказания услуги предоставить F6 вводную информацию путем заполнения опросного листа по форме F6. F6 предоставляет форму опросного листа Заказчику после получения заявки Заказчика на оказание данной услуги в соответствии с Общими условиями.

профилей пользователей иных ОС, файловые таблицы, списки запущенных процессов и т.п., журналы различных СЗИ и иные данные с криминалистически значимой информацией.

2. **Сбор данных для криминалистического анализа.**

   Для сбора данных с систем инфраструктуры (хостов) под управлением ОС семейств Windows, Linux (Unix), macOS F6 формирует перечень необходимых для криминалистического анализа данных и готовит инструменты (скрипты/сценарии, программы, а также инструкции по их запуску) для их сбора. После чего F6 предоставляет Заказчику ссылки на скачивание инструкций и инструментов. Запуск предоставленных инструментов осуществляется Заказчиком самостоятельно в соответствии с предоставленными инструкциями.

   Собранные для анализа данные, выгружаются Заказчиком из его систем и передаются (загружаются) специалистам F6 в корпоративное облачное хранилище F6 по ссылке или иным доступным Заказчику способом (отправка дисков с данными курьером, размещение данных в собственном корпоративном облаке и отправка специалистам F6 ссылки на их загрузку и т.п.).

   По запросу F6 Заказчик также предоставляет выгрузки данных из различных СЗИ и систем учета, образы носителей информации, дампы оперативной памяти и прочие сведения, имеющие отношение к выявленному инциденту.

3. **Внедрение ПО (опционально).**

   Если Заказчик при оказании услуги согласен на внедрение какого-либо ПО, принадлежащего F6 и входящего в программный комплекс XDR, F6 может предоставить Заказчику виртуальные машины или серверное оборудование с предустановленным ПО. ПО будет использоваться для отслеживания подозрительной активности в ИТ-инфраструктуре Заказчика, отправки данных в удаленное хранилище для последующего анализа и блокирования угроз.

   Заказчик обязуется провести работы по внедрению или интеграции ПО в свою ИТ-инфраструктуру совместно с представителями F6.

   Для диагностики текущего состояния ИТ-инфраструктуры и осуществления проактивного поиска угроз необходимо развертывание следующего ПО, принадлежащего F6:

- Сенсоров для анализа сетевого трафика (F6 Network Traffic Analysis). ПО может быть установлено в виде виртуальной машины или программно-аппаратного комплекса.
- EDR-агентов (F6 Endpoint Detection and Response) для мониторинга активности на конечных точках под управлением ОС семейств Windows, Linux (Unix) и macOS.

4. **Проактивный поиск угроз на основе данных из ПО (доступно при внедренном согласно 3 этапу оказания услуги ПО).**

   Собираемые ПО данные также используются для проактивного поиска угроз. Целью поиска является обнаружение сложных угроз, которые могут быть реализованы злоумышленниками с помощью

легитимных инструментов, а также техник уклонения от обнаружения и противодействия криминалистическому анализу.

5. **Криминалистический анализ собранных данных.**

   F6 осуществляет криминалистический анализ данных, собранных с помощью предоставленных инструментов, с целью выявления следов компрометации.

   Анализ собранных данных осуществляется после загрузки Заказчиком всех необходимых для исследования данных и уведомления об этом F6, за исключением случаев обращения Заказчика за услугой по реагированию на инцидент ИБ.

6. **Выявление следов компрометации и их корреляция с данными киберразведки ПО F6 Threat Intelligence.**

   При обнаружении признаков компрометации тех или иных систем F6 формирует и оперативно передает Заказчику список индикаторов компрометации для их дальнейшего поиска в инфраструктуре Заказчика. Совместно с ними предоставляются рекомендации по локализации выявленных угроз. По результатам сканирования сети Заказчик может повторно провести этапы сбора и анализа данных.

   Также на данном этапе F6 проводит корреляцию выявленных сведений с данными киберразведки ПО F6 Threat Intelligence и данными программного комплекса XDR F6.

   При необходимости F6 может запросить дополнительную информацию с целью выявления причин компрометации той или иной системы.

7. **Локализация выявленных угроз.**

   По мере изучения предоставляемых данных и обнаружения среди них сведений об угрозах специалисты F6 в оперативном режиме предоставляют Заказчику рекомендации по их локализации.

8. **Реконструкция действий атакующих на основе имеющихся источников цифровых следов и атрибуция к действующим преступным группам.**

   Если криминалистический анализ позволяет выявить достаточное количество цифровых следов, включая использованные атакующими инструменты и ВПО, то специалисты F6 проводят реконструкцию их действий. Целью этой процедуры является выявление причин компрометации, а также атрибуция выявленной активности к действующим преступным группам (если возможно). Реконструкция включает описание примененных атакующими тактик, техник и процедур.

9. **Анализ ВПО.**

   В случаях обнаружения ВПО F6 проводит его анализ, который позволяет установить:

- его функциональные возможности;

- сведения о его сетевых взаимодействиях и адреса управляющих серверов;
- дополнительные индикаторы компрометации, необходимые для поиска скомпрометированных конечных станций;
- методы закрепления в системе (при наличии).
- В процессе применяются техники статического и динамического анализа.

10. Подготовка отчета.

По результатам оказания услуги F6 готовит отчет[41], который содержит:

- описание проделанных работ и выводы о наличии либо отсутствии признаков компрометации ИТ-инфраструктуры;
- описание выявленных инцидентов (если обнаружено), причин их наступления, индикаторов компрометации и рекомендаций по локализации угроз;
- сведения о компрометации ИТ-инфраструктуры Заказчика, а также упоминания о ней в базе знаний ПО F6 Threat Intelligence;
- описание функциональных возможностей ВПО и инструментов, если таковые выявлены;
- рекомендации по повышению как общего уровня защищенности ИТ-инфраструктуры, так и отдельных ее сегментов, для минимизации рисков наступления подобных инцидентов в будущем.

Требования и ограничения

Заказчик осведомлен и согласен с тем, что:

- Если Заказчику требуется процессуальное оформление инцидента или имеются соответствующие требования регулятора, то перед выполнением процедур удаления данных, восстановления систем и т.д. необходимо соблюсти ряд условий: снять побитовые копии с носителей информации; при необходимости надлежащим образом оформить цифровые улики.
- Возможности по установлению точки первоначальной компрометации и восстановлению полной хронологии инцидента зависят от глубины журналирования событий и деструктивных действий злоумышленников. Вследствие этого обстоятельства инцидента не всегда могут быть установлены и восстановлены в полном объеме.

Срок оказания услуги[42]

Количество исследуемых систем (хостов)	Минимальное количество часов, необходимое для оказания услуги	Минимальный срок оказания услуги (в рабочих днях)	Срок начала оказания услуги

[41] По согласованию Сторон F6 может подготовить отчет на бумажном носителе для предоставления в правоохранительные органы или иные регулирующие организации.

[42] Исполнитель приступает к оказанию услуги в согласованные Сторонами сроки, при условии предоставления Заказчиком Исполнителю всех необходимых для оказания услуги данных.

до 1000 систем	120	15	до 1 месяца
до 3000 систем	160	20	
до 5000 систем	200	25	
до 10000 систем	560	35	
до 15000 систем	640	40	
до 20000 систем	960	60	

Услуга: реагирование на инциденты

Описание услуги

Услуга направлена на локализацию инцидентов информационной безопасности и выявление причин их наступления.

Состав услуги[43]

В рамках услуги F6 может совершать следующие действия:

1. Организация оперативного и своевременного начала услуги по реагированию на инциденты ИБ.

1.1 Регистрация запроса Заказчика.

Заказчик направляет запрос с описанием инцидента контактному лицу F6 по заранее согласованным телекоммуникационным каналам в виде опросного листа. Далее запрос регистрируется и передается команде реагирования на инциденты ИБ - Лаборатории цифровой криминалистики и исследования вредоносного кода F6.

1.2 Первичная консультация Заказчика по техническим вопросам.

F6 по запросу Заказчика дает устную консультацию исходя из вводной информации, предоставляемой Заказчиком в части:

- Целесообразности оказания услуги по реагированию на инцидент ИБ;
- Возможных причин возникновения инцидента ИБ;
- Экстренных технических и организационных мер по реагированию на инцидент ИБ и его локализации.

Особые условия:

- Вводная информация предоставляется Заказчиком в виде опросного листа либо на первичной встрече со специалистами F6, либо перед ней;
- Консультации оказываются при наличии достаточной информации и возможности предоставления дополнительной информации Заказчиком по запросу F6;

[43] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

- Консультации оказываются в рамках компетенций технических специалистов F6;
- При необходимости F6 предоставляет Заказчику необходимые инструменты и инструкции по сбору данных (криминалистических артефактов) для первичного анализа, оценки сложности инцидента ИБ.

1.3 Первичный анализ данных для оценки сложности инцидента ИБ.

В рамках данного этапа услуги F6 совершает следующие действия:

- Проводит предварительный анализ предоставленных Заказчиком данных по инциденту ИБ;
- Оценивает сложность инцидента ИБ;
- Оценивает формат оказания услуги (удаленно или с выездом специалиста(-ов) на территорию Заказчика);
- Запрашивает дополнительную информацию у Заказчика и предоставляет первичные рекомендации, направленные на локализацию инцидента ИБ (при необходимости и если возможно);
- Предоставляет Заказчику ориентировочный срок оказания следующих этапов услуги и предлагает время стартового совещания.

2. Стартовое совещание.

Во время стартового совещания:

- Координатор/менеджер проекта:
- обсуждает детали инцидента ИБ с представителем(-ями) Заказчика;
- предлагает время начала оказания услуги (включая поездки для работы на территорию Заказчика, при необходимости);
- запрашивает дополнительную информацию (если требуется).
- F6 предоставляет Заказчику базовые рекомендации для временного уменьшения последствий инцидента ИБ (если возможно), если таковые по той или иной причине не были предоставлены в рамках этапа 1.3. услуги.
- Заказчик выделяет ответственного специалиста или группу специалистов, которые будут взаимодействовать с группой реагирования F6, а именно собирать необходимые данные для анализа и осуществлять иные действия по требованию F6 внутри инфраструктуры Заказчика в рамках услуги.
- F6 может запрашивать дополнительную информацию о внутреннем расследовании инцидента (если проводилось), топологии сети IT-инфраструктуры, публично доступных сервисах и способов легитимного доступа к ним, системах резервного копирования, виртуализации и средствах централизованного управления ей, конфигурации доменов Active Directory и доверительных отношениях в них, об облачных хранилищах, используемых СЗИ, в

т.ч. системах сбора и регистрации событий безопасности и иные сведения.

3. **Сбор данных для анализа.**

   Для сбора данных с систем инфраструктуры (хостов) под управлением ОС семейств Windows, Linux (Unix), macOS, F6 предоставляет Заказчику ссылки на скачивание инструментов (скриптов/сценариев, программ) для сбора данных, а также инструкции по их запуску. Запуск инструментов на хостах Заказчик осуществляет самостоятельно в соответствии с предоставленными инструкциями.

   В случаях, когда особенности возникшего инцидента не позволяют выполнить сбор необходимой информации согласно предоставленным инструкциям, F6 проводит консультации и дает рекомендации по решению проблемы в сборе данных.

   При отсутствии у Заказчика возможности самостоятельного сбора данных, по согласованию с F6 он может осуществляться специалистами F6 совместно с представителями Заказчика:

- Локально (на территории Заказчика) при непосредственном участии представителей Заказчика, обладающих знаниями об устройстве ИТ-инфраструктуры и правами доступа к ней;
- Удаленно, при наличии возможности безопасной организации удаленного доступа (по оценке специалистов F6), а также при наличии круглосуточной поддержки со стороны представителей Заказчика, обладающих знаниями об устройстве ИТ-инфраструктуры и правами доступа к ней.

С помощью предоставленных инструментов осуществляется сбор следующих данных:

- файловые таблицы, а также списки файлов, имеющиеся на системном диске, журналы файловых систем;
- файлы системного и пользовательских реестров ОС Windows, файлы конфигураций профилей пользователей иных ОС;
- параметры командных интерпретаторов различных ОС;
- журналы событий ОС, а также различных системных и прикладных программ и сервисов, расположенных на целевых системах в каталогах по умолчанию;
- журналы событий антивирусных программ и файлы, отправленные ими в карантин;
- задания планировщиков различных ОС и их списки;
- ярлыки ранее открытых файлов и списки переходов, создаваемых ОС в процессе работы;
- файлы веб-браузеров со сведениями о посещениях веб-ресурсов и о загруженных файлах;
- содержимое каталогов автозагрузки (для ОС Windows), исполняемые файлы запущенных процессов;
- списки запущенных процессов и сетевых соединений;

- криптографические хеш-суммы исполняемых файлов, расположенные в нетипичных (подозрительных по мнению специалистов) каталогах.

В случаях, когда собранных предоставленными инструментами данных недостаточно, F6 вправе дать рекомендации и запросить у Заказчика:

- выгрузки сетевых соединений и дампов сетевого трафика из различного сетевого оборудования;
- выгрузки данных из имеющихся средств защиты информации (SIEM, DLP и иных);
- побитовые копии (RAW) отдельных физических носителей информации и файлы дисков виртуальных машин;
- различные журналы событий, расположенные в нетипичных каталогах, а также выгрузки из них;
- дампы памяти, временные файлы и прочие сведения, имеющие отношение к инциденту ИБ.

4. Криминалистический анализ собранных данных.

F6 проводит комплексный анализ всей доступной информации, включая образцы ВПО, задействованного в инциденте, с целью локализации инцидента, восстановления хронологии событий, а также выявления индикаторов компрометации.

Анализ собранных данных выполняется удаленно на ресурсах F6 в кратчайшие сроки с момента их предоставления. Длительность анализа данных может зависеть от их состояния и доступности (например, данные находятся в зашифрованном или удаленном виде; к данным применялись методы противодействия криминалистическому анализу и т.п.).

Результаты анализа, включая выявленные индикаторы компрометации, оперативно передаются Заказчику. Совместно с ними предоставляются рекомендации по локализации угроз и инцидента.

По запросу Заказчика F6 информирует об актуальном статусе оказания услуги.

В рамках оказания данного этапа услуги F6 также осуществляет анализ ранее собранных Заказчиком данных и производит их сверку с базой индикаторов F6, о результатах чего информирует Заказчика. В результате оказания услуги по данному этапу возможен дополнительный сбор данных и цифровых доказательств.

5. Анализ ВПО

В случаях обнаружения ВПО F6 проводит его анализ с целью выявления:

- его функциональных возможностей;
- сведений о его сетевых взаимодействиях с управляющей инфраструктурой;

- дополнительных индикаторов компрометации, необходимых для поиска скомпрометированных конечных станций;
- Методов закрепления в системе (при наличии).
- В процессе анализа применяются техники статического и динамического анализа.

6. Локализация угроз

По мере изучения предоставляемых данных специалисты F6 в оперативном режиме оповещают Заказчика о выявленных угрозах и предоставляют рекомендации по их локализации.

7. Реконструкция действий атакующих на основе имеющихся источников цифровых следов.

В случаях, если криминалистический анализ позволяет выявить достаточное количество цифровых следов, тактик, техник и процедур атакующих, их инструментов (в т.ч. ВПО), специалистами F6 проводится реконструкция действий атакующих. Также при наличии технической возможности и достаточности сведений, позволяющих провести атрибуцию выявленной нелегитимной активности, проводится атрибуция к действующим преступным группам.

Особые условия:

- Услуга оказывается при наличии технической возможности и целесообразности данной операции с точки зрения затраченного времени и состояния исследуемых систем;
- Услуга не гарантирует полное восстановление утерянной или зашифрованной информации;
- В случае понимания специалистами F6 нецелесообразности продолжения попыток восстановления утерянной или зашифрованной информации, услуга перестает оказываться по согласованию с Заказчиком.

8. Подготовка итогового отчета.

По результатам оказания услуги F6 готовит отчет по реагированию на инцидент ИБ44, который содержит следующую информацию45:

- Обстоятельства инцидента;
- Краткое описание инцидента (обзор);
- Табличное представление тактик, техник и процедур (в соответствии с MITRE ATT&CK), использованных злоумышленниками в инциденте;

[44] По согласованию Сторон F6 может подготовить отчет на бумажном носителе для предоставления в правоохранительные органы или иные регулирующие организации.

[45] В случае отказа от услуги после начала анализа данных и предоставления рекомендаций по сдерживанию, ликвидации и восстановлению последствий инцидента, в отчет будут включены сведения о выявленных событиях инцидента и результаты оперативного анализа, зафиксированные на момент отказа.

	• Реконструкция инцидента – подробное описание инцидента, поэксплуатированных уязвимостей (если возможно), возможные или установленные источники атаки, выявленные адреса сетевой инфраструктуры атакующих, результаты анализа ВПО (если оно было задействовано) и иная информация, касающаяся инцидента; • Индикаторы компрометации; • Рекомендации по повышению уровня защищенности ИТ-инфраструктуры Заказчика и на недопущение повторного наступления подобных инцидентов.
Требования и ограничения	**Заказчик осведомлен и согласен с тем, что:** • Полнота и оперативность предоставляемой F6 информации напрямую влияют на скорость и эффективность реагирования на инцидент ИБ специалистами F6; • Возможности по установлению точки первоначальной компрометации и восстановлению полной хронологии инцидента зависят от глубины журналирования событий и деструктивных действий злоумышленников. Вследствие этого обстоятельства инцидента не всегда могут быть установлены и восстановлены в полном объеме. • F6 не проводит детальный анализ событий, образцов ВПО, следов компрометации, не относящихся к данному инциденту. • Если Заказчику требуется процессуальное оформление инцидента или имеются соответствующие требования регулятора, то перед выполнением процедур удаления данных, восстановления систем и т.д. необходимо соблюсти ряд условий: снять побитовые копии с носителей информации; при необходимости надлежащим образом оформить цифровые улики.
Срок оказания услуги[46]	• Минимальный срок оказания услуги – 5 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 40 часов. • Срок начала оказания услуги - до 2 часов.[47]

Услуга: проверка и оценка готовности к реагированию на инциденты ИБ

Описание услуги	Услуга направлена на оценку всех компонентов инфраструктуры Заказчика, в том числе сотрудников Заказчика, на предмет готовности к реагированию на инциденты ИБ. Проверка затрагивает оценку возможности, наличия и отработанности процедур полного и корректного сбора цифровых доказательств, готовности оперативно остановить инцидент и управлять инфраструктурой в ходе реагирования.

[46] Конкретный срок оказания услуги определяется в зависимости от сложности инцидента и состояния данных.

[47] Срок оказания услуги отсчитывается с момента получения F6 Заявки Заказчика и первого запроса информации специалистами F6 у Заказчика.

Состав услуги[48]

В рамках услуги F6 может совершать следующие действия:

1. **Проверка ИТ-инфраструктуры на предмет готовности к реагированию на инциденты ИБ.**

Данный этап включает проверку следующих компонентов ИТ-инфраструктуры Заказчика:

- источники событий ИБ: журналы DHCP; журналы DNS; журналы сетевого трафика; журналы событий с конечных рабочих станций и серверов (на уровне ОС); журналы EDR-систем; журналы подключений Wi-Fi; журналы подключений VPN; журналы web-access; журналы DLP-систем; журналы антивирусного ПО; журналы использования аутентификационных данных; журналы авторизаций и действий пользователей на бизнес-системах; журналы аудита действий пользователей на серверах виртуальных машин (гипервизоры, облачные системы: AWS, Google Cloud Platform, Yandex Cloud, Azure и др.);анализ источников и производительности SIEM-системы; электронная почта;
- организацию резервного копирования;
- регламенты смены паролей учетных записей, а именно возможности централизованной смены паролей ко всем учетным записям, в т.ч. сервисным/технологическим;
- оценка возможности централизованного запуска сканеров индикаторов компрометации и иных инструментов для получения цифровых доказательств.

Результаты оказания услуги по данному этапу:

Подготовлен раздел отчета со следующими сведениями:

- соответствие готовности к реагированию на типовые инциденты ИБ на основании разработанной специалистами Лаборатории скоринговой системы.
- перечень рекомендаций по настройке или модернизации существующей системы мониторинга событий ИБ Заказчика.

2. **Проверка готовности и компетенций внутренней команды реагирования Заказчика на инциденты ИБ.**

Данный этап оказания услуги включает:

- проверку осведомленности специалистов об актуальных угрозах и способах противодействия им (тестирование);
- проверку навыков владения профильными инструментами для сбора и анализа различных источников криминалистически значимой информации:

[48] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

	• проверку навыков владения SIEM-системами и иными системами мониторинга и управления событиями безопасности (если имеются). **Результаты оказания услуги по данному этапу:** **Подготовлен раздел отчета со следующими сведениями:** • оценка теоретической и практической готовности внутренней команды по реагированию на инциденты; • анализ соответствия метрикам F6 о готовности к реагированию на инциденты ИБ; • перечень рекомендаций по повышению компетенций команды реагирования и улучшению показателей по приведенным метрикам; • перечень рекомендаций по модернизации инструментария, используемого сотрудниками Заказчика для проведения работ по реагированию на инциденты ИБ. **3. Проверка инструкций и регламентов по реагированию на инциденты ИБ (при их наличии у Заказчика).** Данный этап оказания услуги включает в себя проверку имеющихся у Заказчика политик, регламентов, инструкций по реагированию на инциденты ИБ. Кроме того, проводится проверка инструментов, используемого специалистами по реагированию на инциденты ИБ Заказчика, на предмет соответствия лучшим практикам и критериям, подготовленным специалистами F6; **Результаты оказания услуги по данному этапу:** **Подготовлен раздел отчета со следующими сведениями:** • рекомендации по улучшению набора инструментов, использующихся специалистами команды по реагированию на инциденты ИБ Заказчика; • рекомендации по доработке политик, регламентов, инструкций по реагированию на инциденты ИБ.
Срок оказания услуги	• Минимальный срок оказания услуги – 15 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 120 часов. • Срок начала оказания услуги - до 1 месяца.

Услуга: цифровая криминалистика

Описание услуги	Услуга направлена на криминалистическое исследование цифровой информации (осмотры, исследования и экспертизы), сбор и оформление (фиксацию) цифровых доказательств.

Состав услуги[49]

В рамках услуги F6 может осуществлять следующие действия:

1. **Криминалистическое исследование компьютерной информации.**

Данный этап услуги может включать в себя:

- Выявление криминалистически значимых обстоятельств инцидента на основании представленных Заказчиком вопросов и критериев;
- Сбор и анализ цифровых доказательств, необходимых для проведения криминалистического исследования;
- Реконструкцию хронологии событий инцидента и установление возможных причин его возникновения;
- Исследование функциональных возможностей ВПО (сетевые взаимодействия, взаимодействия с ОС) с применением техник статического и динамического анализа;
- Определение потенциальных последствий использования ВПО злоумышленником;
- Решение поисковых задач по заданным критериям Заказчика (ключевые слова, фразы, файлы, эталонные изображения и т.п.);
- Исследование баз данных из различных информационных систем. Реконструкция баз данных;
- Исследование дампов сетевого трафика;
- Исследование дампов оперативной памяти;
- Поиск следов несанкционированного доступа;
- Извлечение и анализ почтовой переписки;
- Исследование мобильных устройств;
- Исследование средств видеорегистрации информации;
- Исследование видеограмм на наличие монтажа;
- Сравнение программных продуктов на предмет плагиата;
- Исследование файлов с повреждённой структурой;
- Восстановление данных с носителей информации и RAID-массивов;
- Оценка полноты объёма выполненных работ по созданию информационно-телекоммуникационных систем или разработке ПО в соответствии с договорами (техническими заданиями);
- Рецензирование заключений экспертов;
- Поиск следов хищения информации. Установление объёма похищенных данных и того какие именно данные были похищены;

Результаты оказания услуги по данному этапу:

- Подготовлены опечатанные объекты исследования;

[49] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

- Подготовлен отчет (заключение специалиста) об оказанной услуге[50], содержащий обоснованные ответы на поставленные Заказчиком вопросы, иные сведения, имеющие отношение к исследованию, и рекомендации по предотвращению подобных инцидентов.

2. Сбор и оформление цифровых доказательств.

Сбор доказательств в форме компьютерной информации проводится с целью юридически значимого и криминалистически корректного изъятия машинных носителей информации, а также копирования данных для дальнейшего криминалистического исследования.

При необходимости для обеспечения юридической значимости информации специалисты F6 выполняют ее сбор и оформление с учетом всех требований законодательства РФ, а также применяют неразрушающие методы копирования информации из информационных систем Заказчика.

В случае оказания данного этапа услуги локально (на территории Заказчика) F6 может совершать следующие действия:

- Выезд специалиста F6 на территорию Заказчика в пределах г. Москвы (продолжительностью не менее 3 (Трех) часов) с целью определения перечня криминалистически значимых носителей информации и/или сведений из информационных систем Заказчика;
- Сохранение и снятие посекторной копии с носителей информации или иных объектов информационных систем Заказчика на представленные заранее Заказчиком носители информации;
- Выгрузка и сохранение данных из информационных систем Заказчика на представленные заранее Заказчиком носители информации;
- Изъятие криминалистически значимых носителей информации в случае невозможности сохранения и снятия посекторной копии с носителей информации или выгрузки и сохранения данных из информационных систем Заказчика;
- Упаковка и опечатывание носителей информации или иных объектов информационных систем Заказчика.

Результаты оказания услуги по данному этапу:

- Подготовлен упакованный и опечатанный носитель информации (1 или несколько), содержащий скопированные в рамках оказания услуги криминалистически значимые данные или изъятый в рамках оказания услуг носитель информации Заказчика.
- Подготовлен комплект документов, подтверждающих факты копирования цифровых данных или изъятия носителей информации, а также их передачу между Сторонами.

[50] Заказчик имеет право предоставлять отчет в правоохранительные, судебные органы, а также в регулирующие деятельность Заказчика организации и государственные (муниципальные) органы.

В случае удаленного оказания данного этапа услуги F6 может совершать следующие действия:

- Удаленное выявление F6 перечня источников криминалистически значимых цифровых данных в информационных системах Заказчика при непосредственном участии уполномоченных сотрудников со стороны Заказчика;
- Копирование Заказчиком выявленных источников криминалистически значимых цифровых данных из информационных систем Заказчика с последующей передачей F6 через информационно-телекоммуникационную сеть по защищенному каналу;
- Фиксация F6 предоставленных Заказчиком источников криминалистически значимых цифровых данных;
- Формирование F6 документов, описывающих процессы идентификации, копирования и фиксации источников криминалистически значимых цифровых данных.

Результаты оказания услуги по данному этапу:

- Подготовлен упакованный и опечатанный носитель информации (1 или несколько), содержащий скопированные в рамках оказания услуги источники криминалистически значимых цифровых данных из информационных систем Заказчика;
- Подготовлен комплект документов, описывающих процессы идентификации, копирования и фиксации источников криминалистически значимых цифровых данных.

3. Привлечение специалиста для дачи пояснений по оказанной услуге.[51]

Привлечение специалистов F6 в качестве свидетелей, специалистов, экспертов для участия в процессуальных действиях или в судах по обстоятельствам, связанным или не связанным с ранее оказанными услугами.

Состав и результат услуги определяются по согласованию Сторон.

Срок оказания услуги

- Минимальный срок оказания услуги – 5 рабочих дней.
- Минимальное количество часов, необходимое для оказания услуги - 40 часов.
- Срок начала оказания услуги - до 1 месяца.

Расследования

Услуга: исследование инцидента информационной безопасности

Описание услуги

Исследование инцидента информационной безопасности направлено на установление инфраструктуры и причастных к инциденту лиц.

[51] Не может составлять менее 3-х часов.

Состав услуги[52]

В рамках услуги F6 может осуществлять следующие действия.

1. Анализ инцидента:

- Анализ исходных данных (образов компьютеров, журналов событий, почтовых ящиков, мессенджеров, интернет-ресурсов, объявлений в сети Интернет, видео-контента и т.д.), предоставленных Заказчиком;
- Опрос представителей Заказчика об инциденте;
- Сбор дополнительных цифровых доказательств по инциденту;
- Выявление индикаторов инцидента и его характерных признаков;
- Установление инфраструктуры, используемой в инциденте;
- Предварительный анализ результатов опроса и полученных данных об инциденте.

Результаты оказания услуги по данному этапу:

Подготовлена справка, содержащая описание и результаты совершенных действий.

2. Исследование инцидента:

- Выявление цифровых идентификаторов с целью определения существенных обстоятельств инцидента;
- Выявление обстоятельств инцидента по выявленным цифровым идентификаторам;
- Содействие в проведении элементов служебного расследования на предмет причастности работников Заказчика к инциденту;
- Установление ролей причастных к инциденту лиц и способов их коммуникации;
- Подготовка детального отчета о совершенных действиях с указанием этапов.

Результаты оказания услуги по данному этапу:

Подготовлен отчет, содержащий описание и результаты совершенных действий.

3. Сопровождение:

- Подготовка технической справки, описывающей способы и этапы получения информации. Такая справка предназначена для предоставления в правоохранительные органы;
- Оформление отчета и его сопровождение специалистами F6 в ходе судебного разбирательства в качестве технических специалистов, а также участие в допросах и судебных заседаниях по данным, указанным в отчете, в качестве технических специалистов.

Результаты оказания услуги по данному этапу:

[52] Конкретный состав услуги согласовывается Сторонами в Заявке Заказчика.

	• Подготовлена техническая справка, предназначенная для предоставления в правоохранительные органы; • Подготовлен отчет, содержащий описание совершенных действий.
Требования и ограничения	**Заказчик проинформирован и согласен с тем, что:** • Сведения и выводы, содержащиеся в отчете, являются результатом анализа данных в рамках оказанной услуги и не могут быть трактованы в качестве прямых обвинений и заявлений о причастности или непричастности третьих лиц к инциденту; • F6 не проводит детальный анализ событий, образцов ВПО, следов компрометации, не относящихся к данному инциденту.
Срок оказания услуги	• Минимальный срок оказания услуги – 5 рабочих дней. • Минимальное количество часов, необходимое для оказания услуги - 24 часа. • Срок начала оказания услуги - до 2 рабочих дней после получения F6 от Заказчика всех Исходных данных.

Тренинг

Услуга: проведение тренинга в сфере обеспечения информационной безопасности

Описание и сроки оказания услуги	Наименования тренингов, программы, форматы проведения и сроки указаны на сайте https://www.f6.ru/cybersecurity-education/. Заявка Заказчика на проведение тренинга должна поступить F6 не позднее, чем за 14 (Четырнадцать) календарных дней до даты проведения тренинга. В ином случае F6 вправе отказать Заказчику в проведении тренинга. В случае дистанционного оказания услуги с помощью сети Интернет F6 предоставляет Заказчику и/или непосредственно участнику тренинга (представителю Заказчика) в срок не позднее 3 (Трех) календарных дней до даты начала проведения тренинга: • Ссылку для подключения к онлайн-платформе, на которой осуществляется трансляция тренинга; • Технические требования к оборудованию и программному обеспечению, необходимому для установки Заказчиком перед началом проведения тренинга. **F6 вправе:** • В одностороннем порядке изменять даты проведения тренинга, предварительно уведомив об этом Заказчика по электронной почте в срок не позднее 3 (Трех) календарных дней до даты начала проведения тренинга; • В случае болезни тренера F6, препятствующей проведению соответствующего тренинга, или записи на тренинг до даты его проведения менее 7 (Семи) участников (для наборных видов тренинга), или наличия технических неполадок, не зависящих от F6,

	в любое время в одностороннем порядке изменять даты проведения тренинга, уведомив об этом Заказчика по электронной почте; • В случае болезни тренера, препятствующей надлежащему проведению тренинга или записи на тренинг до даты его проведения менее 7 (Семи) участников (для наборных видов тренинга) в одностороннем порядке отменить тренинг, уведомив об этом Заказчика по электронной почте в срок не позднее 14 (Четырнадцати) календарных дней до даты начала проведения тренинга. **Заказчик обязуется:** • В срок не позднее 7 (Семи) календарных дней до даты начала проведения тренинга предоставить F6 следующие данные участников Заказчика: фамилию, имя, отчество, должность, наименование Заказчика, адрес электронной почты; • До даты начала проведения тренинга обеспечить соблюдение технических требований, предоставленных F6 по электронной почте; • На дату проведения тренинга обеспечить представителям F6, участвующим в проведении тренинга, доступ на свою территорию и предоставить помещение, пригодное для проведения тренинга (в случае проведения тренинга на территории Заказчика).
Требования и ограничения	**Заказчик заверяет и гарантирует, что:** • Участники Заказчика не будут осуществлять в рамках участия в тренинге действия, направленные на развязывание любого рода конфликтов (в том числе в отношении расовой, религиозной дискриминации), пропаганду причинения вреда жизни и здоровью, пропаганду насилия и массовых беспорядков, унижение чести и человеческого достоинства. Также участники не будут использовать ненормативную лексику, оскорблять иных участников тренинга, осуществлять действий эротического характера, рекламировать какие-либо товары и услуги, размещать ссылки на сторонние ресурсы; • Участники Заказчика обладают навыками, необходимыми для прохождения тренинга. Требования к навыкам указаны в программе тренинга на сайте https://www.f6.ru/cybersecurity-education/. При нарушении Заказчиком указанных заверений и гарантий F6 вправе в одностороннем порядке ограничить доступ участников Заказчика к тренингу вплоть до его окончания, что не будет считаться нарушением обязательств со стороны F6.

3. Прочие условия

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

3.2. 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. 3.1. Специальных условий.

3.3. 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/sphere/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).

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

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