# ТИПОВОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ
# НА ВЫПОЛНЕНИЕ РАБОТ ПО ОЦЕНКЕ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

**Москва, 2022 г.**

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

| Термин / Сокращение | Расшифровка и определение |
|---|---|
| Недопустимое событие | Событие, возникающее в результате действий злоумышленников и делающее невозможным достижение операционных и стратегических целей или приводящее к длительному нарушению основной деятельности организации. |
| Brute Force | Атака методом полного перебора |
| SQL | Structured Query Language - язык структурированных запросов |
| XML | eXtensible Markup Language - расширяемый язык разметки. Используется для хранения и передачи данных |
| LFI | Local File Inclusion - подключения локальных файлов с выводом для чтения на стороне сервера |
| RFI | Remote file include - удалённое выполнение кода на сервере. |
| RCE | Remote code execution - удалённое внедрение кода на сервере |
| XSS | Cross-Site Scripting - межсайтовый скриптинг |
| SMTP | Simple Mail Transfer Protocol - простой протокол передачи почты |
| SSI | Server Side Includes - включения на стороне сервера |
| LDAP | Lightweight Directory Access Protocol - протокол прикладного уровня для доступа к службе каталогов |
| XQuery | язык запросов и функциональный язык программирования, разработанный для обработки данных в формате XML |
| HTTP | HyperText Transfer Protocol – протокол передачи гипертекста |
| CSRF | Cross-site request forgery - межсайтовая подделка запроса |

## 1. ОБЩИЕ СВЕДЕНИЯ

### 1.1.Полное наименование выполняемых работ

Работы по оценке уровня (состояния) защищенности информационной инфраструктуры (далее – Работы, Оценка защищенности). Работы включают в себя два этапа:

– Оценка защищенности;

– поиск успешных следов компрометации информационной инфраструктуры злоумышленником.

### 1.2.Заказчик и Генеральный заказчик

### 1.3.Исполнитель

### 1.4.Место выполнения работ

Работы выполняются на территории Исполнителя и объектах Заказчика, в которых будет предоставлен доступ к информационным системам.

### 1.5.Сроки выполнения работ

### 1.6.Порядок оформления и предъявления заказчику результатов работ

Результаты работ по Оценке защищенности, отчетные документы оформляются и предъявляются Заказчику. В свою очередь Заказчик должен предоставить результаты Правительству Российской Федерации, а также во ФСТЭК и ФСБ России по запросу.

Результаты Работ оформляются Актами сдачи-приемки выполненных работ по этапу.

Все отчетные документы предоставляются в бумажном и в электронном виде.

Все отчетные материалы должны соответствовать требованиям согласно разделу 6 «Требования к отчетной документации».

## 2. ЦЕЛИ И ЗАДАЧИ ВЫПОЛНЕНИЯ РАБОТ

Целью выполнения работ является получение достоверных сведений об уровне (состоянии) защищенности инфраструктуры от реализации недопустимых событий, а также выработка маршрутной карты по модернизации информационной инфраструктуры.

В рамках выполнения работ по Оценке защищенности необходимо решить следующие задачи:

– выявление и консолидация стратегических рисков (недопустимых событий) информационной безопасности;

– выявление уязвимостей информационной инфраструктуры, которые могут быть использованы внешними и внутренними нарушителями для осуществления несанкционированных действий, направленных на нарушение свойств конфиденциальности, целостности, доступности обрабатываемой информации, а также технических средств обработки информации, в результате которых может быть нарушен их штатный режим функционирования, что приведет к реализации недопустимых событий;

– выявление недостатков применяемых средств защиты информации и программных обеспечений, а также оценка возможности их использования нарушителем;

– проверка практической возможности использования уязвимостей (на примере наиболее критических);

– получение оценки текущего уровня защищенности на основе объективных свидетельств;

– разработка маршрутной карты по модернизации информационной инфраструктуры.

## 3. ОРГАНИЗАЦИОННЫЕ РАМКИ ПРОЕКТА

Все действия Исполнителя, которые могут привести к нарушению функционирования или другим негативным последствиям для Заказчика и подведомственных учреждений, согласовываются с Заказчиком заблаговременно.

После выполнения работ все средства проведения Оценки уровня защищенности, применявшиеся в рамках выполнения работ, удаляются из инфраструктуры.

Исполнитель предоставляет полную информацию о действиях, выполнявшихся в ходе Оценке защищенности, применявшихся методах атаки, выявленных недостатках и причинах, результатах использования наиболее серьезных недостатков и объективных свидетельствах, подтверждающих как наличие недостатков, так и результаты их использования специалистами Исполнителя.

Исполнитель обязан во время проведения работ, а также после их выполнения обеспечить защиту сведений, полученных в рамках выполнения работ по данному ТЗ, в соответствии с законодательством Российской Федерации.

## 4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ

В целях проведения Оценки защищенности Исполнитель должен выполнить следующие виды работ:

– создание, совместно с Заказчиком, реестра недопустимых событий;

– оценка возможности реализации недопустимых событий путем моделирования целевых атак;

– оценка мер противодействия моделированию атак со стороны системы защиты информации информационной инфраструктуры Заказчика;

– разработка маршрутной карты по модернизации информационной инфраструктуры с целью повышения уровня защищенности;

– разработка отчетных материалов в соответствии с требования описанными в разделе 6 «Требования к отчетной документации».

Сроки выполнения работ описаны в разделе 5 «Сроки выполнения работ» настоящего технического задания.

### 4.1. Требования к обеспечению процесса проведения Оценки защищенности

Для обеспечения выполнения работ по Оценке защищенности Заказчик предоставляет подписанное авторизационное письмо с описанием внешнего периметра информационной инфраструктуры, путем перечисления внешних сервисов компании, подтверждая факт правообладания данными ресурсами.

Заказчик обеспечивает Исполнителя беспрепятственной возможностью выполнять работы в режиме 24/7 на протяжении всего срока реализации Оценки защищенности.

Исполнитель имеет право выполнять работы с любых IP-адресов.

Дополнительные ограничения могут быть согласованы в рабочем порядке.

### 4.2. Типы нарушителя

В рамках выполнения работ по Оценке защищенности должен моделироваться тип потенциального злоумышленника – нарушитель, не имеющие права доступа в контролируемую (охраняемую) зону (территорию) и не имеющий физического доступа к средствам автоматизации оцениваемой информационной инфраструктуры.

При определении и оценки возможностей внешних и внутренних нарушителей, Исполнитель должен руководствоваться Методикой оценки угроз безопасности информации» утвержденной ФСТЭК России 5 февраля 2021 г.

### 4.3. Требования к Оценке защищенности периметра информационной инфраструктуры

Исполнитель совместно с Заказчиков формирует и согласовывает «Реестр недопустимых событий» путем интервьюирования ответственных лиц.

Оценка возможности реализации недопустимых событий проводится путем моделирования целевой атаки на инфраструктуру Заказчика, включая следующие действия:

- сбор информации об инфраструктуре для последующего анализа и уточнения областей поиска уязвимостей;
- получение информации о топологии веб-приложений, используемых решений, версиях программного обеспечения, логике работы;
- определение текущего уровня защищённости;

- сканирование узлов сетевого периметра;
- идентификация уязвимостей сетевых служб. Должен быть осуществлен анализ данных, полученных в результате сканирования доступных ресурсов. Должны быть выявлены возможности доступа к ресурсам с использованием интерфейсов управления, удаленного доступа или доступа к СУБД, которые не должны быть доступны пользователям сети, в которой выполняется работа. Должны быть выявлены сетевые службы, использование которых позволяет перехватывать сетевой трафик или осуществлять другие атаки;
- анализ защищенности инфраструктурных служб и приложений (DNS, электронная почта и т. д.). Должно быть установлено наличие или отсутствие уязвимостей инфраструктурных служб и приложений;
- поиск и анализ информации из открытых источников, содержащей «чувствительные» сведения, способствующие проведению атак на рассматриваемые ИС (информация из баз утечек аутентификационных данных, информация о выявленных ранее уязвимостях, конфигурационные файлы и файлы журналов аудита, размещенные на общедоступных ресурсах и др.);
- оценка защищенности сети от атак на канальном уровне. Должно быть установлено наличие или отсутствие недостатков в реализации сетевой инфраструктуры, а также в использовании протоколов канального и сетевого уровней, которые могут быть использованы для проведения атак;
- подбор паролей. Должен быть осуществлен подбор словарных паролей пользователей (выбор словаря осуществляется Исполнителем с учетом требований политики блокировки учетных записей ИС);
- анализ технологий и средств защищённого обмена информацией между пользователями;
- определение возможных векторов атак на основании выявленных уязвимостей;
- проверка возможных векторов атак реализации недопустимых событий.

В рамках выполнения работ по оценке защищенности периметра должны быть решены следующие задачи:

- проверка возможности эксплуатации наиболее опасных уязвимостей с целью выхода за границы заданного сегмента ИС. Должна быть установлена возможность или невозможность получения доступа специалистами Исполнителя к критически важным ИС. Данный этап заканчивается проверкой возможности получения доступа к одному или нескольким компонентам ИС или исчерпанием Исполнителем применимых методов развития атаки.
- сбор информации. Должен быть составлен перечень узлов внутренней сети, доступных из определенного Заказчика и подведомственных учреждений для выполнения работ сегмента сети ИС. Должен быть проведен анализ механизма получения IP-адреса в сети и возможности подключения сторонних устройств. Должен быть осуществлен анализ сегментации сети;
- инвентаризация узлов, доступных из текущего сегмента ИС, без сканирования на наличие уязвимостей, определение типов устройств, операционных систем, приложений по реакции на внешнее воздействие. Должен быть составлен перечень идентифицированных сервисов на узлах, вошедших в границы выполняемых работ;
- выявление недостатков в управлении доступом. Должны быть выявлены ресурсы, к которым удалось получить доступ с использованием согласованного вектора атаки.

### 4.3.1. Требование к Оценке защищенности веб-приложениий

В процессе выполнения работ должна осуществляться проверка наличия следующих уязвимостей:

- некорректная обработка пользовательского ввода, которая позволяет проводить следующие виды атак:
  - внедрение операторов языка SQL (англ. SQL injection), в том числе межмодульное (англ. Second order);
  - межсайтовое выполнение сценариев (Cross-Site Scripting);
  - подделка межсайтового запроса (Cross-Site Request Forgery);
  - включение локальных и удаленных файлов (англ. LFI/RFI/RCE);
  - внедрение кода на языке, интерпретируемом на стороне клиента (англ. XSS), в том числе межмодульное (англ. Stored) и клиентское (англ. DOM-based);
  - внедрение команд, интерпретируемых средой выполнения (англ. Eval injection);
  - внедрение команд, интерпретируемых ОС сервера (англ. OS command injection);
  - внедрение SMTP-команд;
  - внедрение директив SSI;
  - внедрение конструкций языка запросов LDAP;
  - внедрение конструкций языка запросов XPath/XQuery;
  - внедрение разметки на языке XML;
  - внедрение заголовков (Header Injection), в том числе позволяющие разделить HTTP-ответ;
  - подключение внешних XML-сущностей (англ. XML External Entity);
  - прочие атаки, целью которых является выполнение кода на стороне сервера;
  - атака на переполнение буфера применяемых программных и программно-аппаратных компонентов ИС;
- небезопасная реализация загрузки пользовательских файлов на сервер (англ. Unrestricted Upload of File with Dangerous Type);
- отсутствие проверки или некорректная проверка привилегий пользователя при доступе к закрытым функциям или ресурсам (англ. Insufficient authorization);
- ошибки в протоколе проверки подлинности пользователей (англ. Insufficient authentication);
- уязвимости в процедуре восстановления доступа при утере учетных данных (англ. Insufficient password recovery);
- уязвимости в организации безопасного соединения (англ. Insufficient Transport Layer Protection);
- уязвимости, связанные с некорректным управлением сеансами (англ. Insufficient Session Expiration);
- возможность несанкционированного выполнения запросов от имени пользователей (англ. CSRF);
- возможность вызвать отказ в обслуживании (англ. Denial of Service) без применения методов валовой посылки запросов;

- некорректная обработка исключительных ситуаций, приводящая к утечке информации о приложении (англ. Information Leakage);
- выявление общеизвестных уязвимостей в ИС;
- выявление ошибок конфигурации в ИС;
- поиск уязвимостей в ИС, связанных с некорректной обработкой входных данных от пользователей;
- выявление уязвимостей, связанных с логикой работы ИС;
- выявление других свойств ИС, негативно влияющих на безопасность (hardening);
- прочие ошибки, позволяющие изменить логику работы ИС.

## 5. СРОКИ ВЫПОЛНЕНИЯ РАБОТ

Сроки выполнения работ, результаты (отчетные документы) приведены в таблице №1.

**Таблица №1**. Сроки выполнения работ.

| № п/п | Содержание работ | Сроки | Результат (отчетные документы) |
|---|---|---|---|
| 1 | – | | 1. |

## 6. ТРЕБОВАНИЯ К ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

Комплект отчетной документации должен быть предоставлен Заказчику в двух экземплярах (один утвержденный экземпляр возвращается Исполнителю) и в одном экземпляре в электронном виде на оптическом носителе (CD диск), не поддерживающем изменение информации.

Вся разрабатываемая отчетная документация должна быть выполнена на русском языке.

Комплект отчетной документации состоит из аналитического и технического отчета.

Для предоставления объективной оценки выполненных работ Заказчик и Исполнитель обязаны предоставить Правительству Российской Федерации, а также по запросу во ФСТЭК и ФСБ России аналитический отчет Аналитический отчет по Оценке защищенности;

### 6.1. Требования к содержанию «Аналитический отчет по Оценке защищенности»

По результатам выполнения этапа «Оценка защищенности», Исполнитель и Заказчик должны подготовить отчет, содержащий следующие разделы:

- Оценка уровня защищенности;
- реестр недопустимых событий, включающий описание пороговых значений и критериев реализации;
- общее количество ИС в инфраструктуре, количество целевых ИС;
- оценка реализуемости недопустимых событий;
- перечень ограничений, наложенных в рамках реализации работ по Оценке защищенности, включая технические и организационные;
- оценка мер по противодействию моделированию атаки со стороны Заказчика;
- резюме Исполнителя с указанием квалификации сотрудников, привлекаемых к реализации Оценки защищенности, а также описание релевантного опыта по выполнению Оценки защищённости;
- описание цели последующей Оценки защищенности, срок проведения, обновленный реестр негативных последствий.

Отчет по Оценке защищённости подписывается со стороны Заказчика Заместителем руководителя, ответственным за обеспечение информационной безопасности, а также со стороны Исполнителя Главным экспертом, ответственным за выполнение текущей Оценки Защищенности, и Генеральным директором.

### 6.2. Требования к содержанию «Технический отчет по Оценке защищенности»

По результатам выполнения этапа «Оценка защищенности» Исполнитель предоставляет Заказчику Технический отчет, содержащий следующие разделы:

- общие сведения о проведенной Оценке защищенности;
- реестр недопустимых событий со статусом реализованности;
- журнал действий, содержащий следующие сведения: идентификатор субъекта, идентификатор объекта, дату/время активного воздействия, тип действия, описание действия, результат действия;
- результаты проведенных проверок;
- оценку состояния защищенности информационной системы Заказчика;
- перечень и описание существующих угроз;

- графическое отображение основных выявленных векторов атак с оценкой сложности их реализации;
- описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, описание возможных последствий реализации выявленных уязвимостей;
- перечень скомпрометированных в рамках работ компонентов информационной инфраструктуры;
- результаты эксплуатации уязвимостей, приводящих к реализации недопустимых событий;
- описание успешных следов компрометации информационной инфраструктуры, в случае обнаружения.

## 7. ТРЕБОВАНИЯ К ГАРАНТИИ КАЧЕСТВА

Срок предоставления гарантии качества выполненных работ составляет 12 месяцев со дня подписания документа о приемке выполненных работ (оказанных услуг).

Исполнитель в течение срока предоставления гарантии должен обеспечить своевременное (в срок не более 10 рабочих дней после предоставления Заказчиком всей необходимой для устранения ошибок информации) устранение недочетов и ошибок, выявленных после выполнения работ.

Факт регистрации заявки о гарантийном случае подтверждается Исполнителем письмом в адрес ответственного представителя Заказчика, в котором указывается дата и время принятия заявки в работу.

## 8. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ

В соответствии с законодательством (Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации») организация, выполняющие работы по анализу защищенности ИС должна обладать действующей лицензии Федеральной службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, включая услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

Исполнитель должен обладать необходимыми кадровыми ресурсами соответствующей квалификации для реализации данной работы, а именно:

- иметь в штате не менее 20 специалистов по анализу защищенности
- иметь в штате не менее 3 архитекторов информационной безопасности

Квалификация специалистов и архитекторов информационной безопасности подтверждается наличием профильного образования и опытом реализации не менее 10 аналогичных проектов.

| | |
|---|---|
| **от Заказчика:** | **от Исполнителя:** |
| Заместитель генерального директора | Генеральный директор |
| **_____ /ФИО /** | **_____ /ФИО/** |
| **М.П.** | **М.П.** |