**ОПРОСНЫЙ ЛИСТ ПО
ТЕХНИЧЕСКОМУ АУДИТУ БЕЗОПАСНОСТИ**

**ОБЩИЕ СВЕДЕНИЯ**

|  |
| --- |
|  |
| Наименование организации |  |
|  |
| Контактное лицо |  |
|  |
| Телефон |  |
|  |
| Email |  |
|  |
| Дата заполнения |  |
|  |

|  |  |
| --- | --- |
| 1. Цель проведения
 | обязательно |
|  |
| [ ]  Требования законодательства о защите информации в государственных информационных системах (ФЗ-149, Приказ ФСТЭК России №17)[ ]  Требования Положения ЦБ РФ 719-П/683-П об анализе уязвимостей в прикладном ПО (ОУД4)[ ]  Требования Положения ЦБ РФ 719-П/683-П о ежегодном тестировании на проникновение и анализе уязвимостей[ ]  Оценка действующей системы информационной безопасности[ ]  Требования партнеров |
| [ ]  Другое |  |
|  | *Указать* |
| [x]  *- выбрано;* [ ]  *- не выбрано* |
|  |
|  |
| 1. Тестированию подлежит:
 | обязательно |
|  |
| [ ]  **Внешние IP-адреса** (Внешний пентест) |  |
|  | *Указать количество IP-адресов* |
| [ ]  Включая стресс-тест |  |
|  | *Указать количество IP-адресов для стресс-теста* |
|  |  |
|  |  |
| [ ]  **Внутренняя инфраструктура, удаленно** (Удаленный внутренний пентест) |  |
|  | *Указать общее количество хостов* |
|  |  |
|  |  |
| [ ]  **Внутренняя инфраструктура, очно** (Очный внутренний пентест) |  |
|  | *Указать общее количество хостов* |
| [ ]  Включая тест Wi-Fi |  |
|  | *Указать количество точек доступа* |
|  |  |
|  |  |
| [ ]  **Социальная инженерия** |  |
|  | *Укажите формат (очно, дистанционно, оба формата)* |
|  |  |
|  | *количество целевых групп и/или сотрудников* |
| [ ]  Исполнителю необходимо самостоятельно собрать сведения о сотрудниках  Заказчика (OSINT) |
| [ ]  Исполнителю будут предоставлены сведения о сотрудниках Заказчика |
|  |
|  |

|  |  |
| --- | --- |
| Тестированию подлежит (продолжение): | обязательно |
|  |
| [ ]  **Приложение:** |
|  |
| [ ]  Мобильное приложение |  |
|  | *Указать платформу приложения* |
| [ ]  WEB-приложение |  |
|  | *Указать URL* |
| [ ]  Иное |  |
|  | *Описание* |
|  |  |
|  |  |
| [ ]  **Код программного обеспечения** (AppSec) |  |
|  | *Указать объем в Mb* |
|  |
| Используемые языки программирования (Java/PHP/Python/JavaScript/C#/…): |

|  |
| --- |
|  |
|  |
| **Язык программирования** | **Количество строк** |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |

|  |
| --- |
|  |
|  |
| Опишите используемый стек технологий (фреймворки, библиотеки, СУБД, компиляторы. Например: библиотеки jQuery, Bootstrap и Slick, на платформе Angular, Vue.js и React.js; технологии JavaScript, Ionic, Cordova, PhoneGap, Xamarin и т.п.): |
|  |
|  |
| *Описание* |
|  |
|  |
|  |
| 1. Каким образом организована внутренняя инфраструктура (только для тестирования внутренней инфраструктуры):
 |
|  |
| [ ]  Все компьютеры находятся в одном сегменте сети |
|  |
| [ ]  Имеется несколько сегментов. Все компьютеры «видят друг друга» |  |
|  | *Укажите количество сегментов* |
| [ ]  Имеется несколько сегментов. Доступ между сегментами органичен |  |
|  | *Укажите количество сегментов* |
| [ ]  Другое |  |
|  | *Указать* |
|  |
| [ ]  Затрудняюсь ответить |
|  |

|  |
| --- |
| 1. Используются ли в границах исследования службы каталогов? (только для тестирования внутренней инфраструктуры)
 |
|  |
| [ ]  **Да, используются** |
|  |
| [ ]  Active Directory |
|  |
|  |
| [ ]  Другое |  |
|  | *Указать* |
| [ ]  Затрудняюсь ответить |
|  |
|  **При этом** |
|  |
| [ ]  Все компоненты в едином Домене |
|  |
| [ ]  Используется нескольковзаимосвязанных Доменов |  |
|  | *Укажите количество доменов* |
|  |
| [ ]  Используется нескольконесвязанных Доменов |  |
|  | *Укажите количество доменов* |
|  |
| [ ]  **Нет, службы каталогов не используются** |
|  |
| [ ]  **Затрудняюсь ответить** |
|  |
|  |
| 1. Глубина анализа
 | обязательно |
|  |
| [ ]  Анализ уязвимостей без эксплуатации (Анализ защищенности)[ ]  Анализ уязвимостей с попыткой эксплуатации (Pentest)[ ]  Комплексный анализ безопасности организации путем моделирования действий злоумышленника с использованием программных, технических, физических и социотехнических методов с эксплуатацией уязвимостей независимо от природы возникновения с реализацией векторов атак до получения максимального уровня доступа. В отличие от предыдущих подразумевает комплексное тестирование организации, а не только информационной системы. В него входит тестирование физической защиты, подключение несанкционированных устройств, разбрасывание носителей с вредоносным ПО и прочее (RedTeam) |
|  |
|  |
| 1. Формат проведения технического аудита безопасности
 | обязательно |
|  |
| [ ]  **Black Box** (метод «чёрного ящика») — предоставляются только целевые IP-адреса, либо только скомпилированное приложение[ ]  **Gray Box** (метод «серого ящика») — предоставляются дополнительные данные по запросу, но без учетных данных администратора[ ]  **White Box** (метод «белого ящика») — предоставляются дополнительные данные по запросу, включая учетные данные администратора, исходные коды |
|  |
|  |
| 1. Тип имеющихся СЗИ (антивирусы, средства корреляции (SIEM), DLP и пр.), (не указывается в случае Red Team, AppSec, Black Box)
 | обязательно |
|  |
|  |
| *Указать* |
|  |
|  |

**ИНЫЕ УСЛУГИ**

|  |
| --- |
|  |
| 1. Желаемый перечень сопутствующих работ
 |
|  |
| [ ]  Анализ платежного ПО по ОУД4[ ]  Разработка модели угроз по новой методике ФСТЭК |
|  |
|  |
| 1. Желаемый перечень иных работ
 |
|  |
| [ ]  Приведение в соответствие требованиям 716-П[ ]  Аудит организации в направлении обработки/защиты персональных данных[ ]  Аудит на соответствие требованиям 719-П, 683-П, 757-П, 747-П, иных источников требований ЦБ/Приведение в соответствие требованиям 719-П, 683-П, 757-П, 747-П, иных источников требований ЦБ[ ]  Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580[ ]  Независимая внешняя оценка SWIFT[ ]  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» |
|  |
|  |
| 1. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ
 |
|  |
| [ ]  Планируется ли поставка решений ИБ/ИТ?[ ]  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ? |
|  |
| Какие решения по ИБ/ИТ вами рассматриваются? |  |
|  | *Указать* |
|  |
|  |

Благодарим за уделенное время!