

# Последовательность действий ИЛ при проведении испытаний ПО на соответствие требованиям ИБ

## ▼ I. Приём объектов для испытаний

### ▼ А. Описание программы (проверка наличия следующих сведений):

#### ▼ 1) Общие сведения о ПО:

- - Название и версия ПО;
- - Сведения о составе ПО (с указанием контрольных сумм файлов, входящих в состав ПО);
- - Сведения о среде функционирования ПО, языке программирования, среде разработки, СУБД, ОС;
- - Сведения о назначении и области применения ПО;
- - Ограничения при применении ПО и минимальные конфигурации необходимых для инсталляции и функционирования ПО технических средств;
- - Перечень внешних серверов, с которыми осуществляется связь при инсталляции и функционировании ПО;
- - Виды информации, передаваемой и принимаемой с внешних серверов.

#### ▼ 2) Описание архитектуры ПО:

- - Графическая блок-схема клиент-серверной информационной системы;
- - Описание каждой основной части (модуля) клиент-серверной информационной системы;
- - Описание взаимосвязей клиент-серверной информационной системы с другими информационными системами (используемые протоколы, порты, интерфейсы взаимодействия, а также передаваемые данные).

#### ▼ 3) Описание базы данных:

- - Тип и архитектура БД;

- - Графическая схема связей БД (в случае использования нескольких БД) и таблиц;
- - Описание каждой таблицы и содержания данных хранимого объекта.
- ▼ 4) Описание исходного кода ПО:
  - - Структура исходного кода;
  - - Описание компонентов;
  - - Описание файлов по каждому компоненту;
  - - Описание функции сетевого взаимодействия.
- ▼ В. Руководство администратора (проверка наличия следующих сведений):
  - - Наименование и версия ПО;
  - - Наименование организации - разработчика ПО;
  - - Юридический адрес организации - разработчика ПО;
  - - Описания методов, приемов и правил эксплуатации, относящихся к предоставляемым администраторам функциональным возможностям ПО.
- ▼ С. Руководство пользователя (проверка наличия следующих сведений):
  - - Наименование и версия ПО;
  - - Наименование организации - разработчика ПО;
  - - Юридический адрес организации - разработчика ПО;
  - - Описания методов, приемов и правил эксплуатации, относящихся к предоставляемым пользователям функциональным возможностям ПО.
- ▼ D. Исходный код ПО (проверка комплектности):
  - - проверка соответствия количества, наименования и размеров всех файлов, указанных в описании ПО, для всех подсистем, частей, компонентов, модулей.
- ▼ E. Исполняемые файлы (проверка наличия в пользовательском интерфейсе следующих сведений):
  - - наименование и версия ПО;
  - - наименование организации-разработчика ПО;
  - - наименование страны разработчика ПО.
- ▼ F. Тестовый стенд
  - - проверка комплектности согласно минимальным требованиям, указанным в Описании программы;

- - наличие учетной записи к каждому типу роли пользователей (включая доступ с правами администратора).

## ▼ II. Анализ исходного кода с помощью анализатора на основе методики Ts 28189200-07:2021

- A. Контрольная компиляция и сборка
- B. Сравнение скомпилированную ПО с предоставленным ПО
- C. Сканирование исходного кода ПО на уязвимость с помощью анализатора
- D. Анализ в ручном режиме исходного кода ПО на соответствие с его описанием на уровне файлов
- E. Анализ в ручном режиме исходного кода ПО на соответствие с его описанием функций сетевых взаимодействий
- F. Отсутствие избыточных исходных текстов и файлов
- G. Анализ полученных результатов

## ▼ III. Выявление сетевых активностей ИС (период проверки примерно от 1 до 3 месяцев) с помощью «песочницы»

- A. Установка и запуск исполняемых файлов
- ▼ B. Проверка функционала ИС (на основе методики Ts 28189200-06:2021):
  - - Анализ технической документации;
  - - Проверка соответствия пароля установленным требованиям;
  - - Проверка отсутствия возможности входа в систему без пароля;
  - - Проверка отсутствия возможности входа в систему с паролем «по умолчанию»;
  - - Проверка возможности входа в систему с правами администратора;
  - - Проверка фиксации информации о большом количестве запросов на вход в систему;
  - - Получение и сравнение контрольной суммы исполняемых файлов (для ПО на скомпилированных языках) или архива исходного кода в формате ZIP (для ПО на интерпретируемых языках);
  - - Проверка резервного копирования и восстановления системы или базы данных;
- C. Анализ выявленных сетевых активностей

## ▪ IV. Составление Отчета по результатам испытаний

- **V. Предоставление Заявителю Отчета для дальнейшего устранения выявленных уязвимостей и несоответствий**
- **VI. Повторное испытание ПО после устранения Заявителем выявленных уязвимостей и несоответствий**
- **VII. Оформление, утверждение и предоставление в ОС ИКТ Протоколов испытаний**