**Программа и методика испытаний**

автоматизированной системы (процессов/интеграционных решений)

**test\_system\_nlmk**

на соответствие требованиям по информационной безопасности

**Версия \_.\_**

# Объект испытаний

Объектом испытаний является автоматизированная система (процесс/интеграционное решение) **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, краткое наименование – , далее – АС, развернутая в соответствии с ОТАР и иной проектной и эксплуатационной документацией, перечисленной в п. 2.

# Перечень предъявляемой на испытания документации:

* Анкеты с описанием АС для подготовки требований по ИБ;
* БТ
* ОТАР
* Ролевая модель;
* Программа и методика испытаний (настоящий документ);
* Руководство администратора ИБ;
* Документы и сертификаты, необходимые для выполнения требований PCI SSC;
* Другая дополнительная документация.

# Общие положения

Целью проведения испытаний является проверка соответствия АС *(процесса/интеграционного решения)*  предъявленным к ней требованиям по информационной безопасности.

Для проведения испытаний в АС создаются тестовые пользователи, которым назначаются следующие роли:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование роли** | **Назначаемые ей права**  **(в терминах системы)** | **Примечание** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Испытания проводятся по адресу *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*в тестовой среде.

# Условия и порядок проведения испытаний

К испытаниям допускается АС, полностью разработанная и настроенная в соответствии с предъявленными к ней требованиями, изложенными в БТ и ОТАР, с полным комплектом документации, перечисленной в п.2, протестированная Исполнителем в т.ч. в части ИБ. Предъявление АС на испытания по ИБ означает, что все условия, перечисленные в этом пункте, выполнены.

Испытания проводятся путем последовательного выполнения действий в соответствии с методикой испытаний, представленными в Приложении № 1 к настоящей методике.

Испытания считаются успешно завершенными, если выполнены все действия по методике проверки, отсутствуют критичные замечания, а количество некритичных не превышает 10% от общего числа требований. Если в рамках ПСИ ИБ проводятся только интеграционные испытания, то количество некритичных замечаний не должно превышать 20% от общего числа требований.

# Отчетность

По завершении испытаний Исполнителем (Менеджером качества АС) оформляется протокол испытаний.

Приложение № 1

# Программа и методика испытаний автоматизированной системы «test\_system\_nlmk» на соответствие требованиям по информационной безопасности

По завершении проверки каждого требования необходимо убедиться в наличии и корректности отображения записей в журналах аудита о выполненных действиях, если методика подразумевает возникновение таких записей. Отсутствие записей или их некорректное отображение является критичной ошибкой для всех требований.

Требование считается невыполненным, если хотя бы одна из перечисленных критичных ошибок возникает в процессе проверки.

| **№ п/п** | **Код** | **Формулировка требования** | **Методика проверки1** |
| --- | --- | --- | --- |
|  | **AR** | **Архитектура и Дизайн** |  |
|  | AR1 | Сторонние компоненты и библиотеки, используемые для разработки приложения должны быть описаны в документации. Использование компонентов с известными уязвимостями должно быть исключено. |  |
|  | AR2 | Для работы в одном приложении внутренних и внешних пользователей должны использоваться различные инстансы приложения. |  |
|  | AR3 | Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями. |  |
|  | AR4 | Все данные загружаемые в систему должны быть получены из довернных источников. Если исользуются данные из недоверенных источников(например, сторонние Java скрипты) они должны запускаться в iFrame с параметром Sandboxing |  |
|  | AR8 | Реализован механизм принудительных обновлений мобильного приложения |  |
|  | AR6 | Проверки безопасности должны быть реализованы как на клиентской части приложения так и на бэкенде |  |
|  | AR5 | Необходимо использовать правила для линтера, направленные на проверку безопасности кода |  |
|  | **RE** | **Технические. Защита клиентской части** |  |
|  | RE4 | Приложение обнаруживает и реагирует на наличие на устройстве широко используемых инструментов и фреймворков для реверс инжиниринга |  |
|  | RE6 | Приложение обнаруживает и реагирует на изменение своего кода и данных в его области оперативной памяти |  |
|  | **PI** | **Технические. Взаимодействие с ОС** |  |
|  | PI8 | Десериализация объектов, если она есть, реализована с использованием безопасного API сериализации. |  |
|  | **PR** | **Процессные** |  |
|  | PR3 | После формирования требований по защите информации должна быть проведена встреча по их обсуждению | Для Android: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing- Platform-Interaction.md Для iOS: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md |
|  | PR4 | Должно быть проведено моделирование угроз |  |
|  | PR6 | Для приложения должен быть проведен анализ защищенности. Для проведения работе необходимо: выделить бюджет, предоставить учетные записи, схему стенда, стабильно работающий стенд и реквизиты доступа в систему учета ошибок. |  |
|  | PR5 | До развертывания приложения в продуктовой среде должно быть проведено тестирование приложения на предмет выполнения требований по защите информации |  |
|  | PR8 | Перед переводом в продуктовый контур должно быть проведено как тестирование нового приложение, так и систем, доработанных для интеграции с ним. | Для Android: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing- Platform-Interaction.md Для iOS: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md |
|  | PR7 | Должен быть проведен статический анализ приложения. Для внешней разработки - предоставлены результаты данного анализа. |  |
|  | **SM** | **Технические. Управление сессиями** |  |
|  | SM11 | Если в приложении используется управление сессиями с сохранением состояния(stateful), то бэкэнд использует случайным образом сгенерированные идентификаторы сессии для аутентификации клиентских запросов. При этом учетные записи пользователей не пересылаются | Для Android: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing- Platform-Interaction.md Для iOS: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md |
|  | SM12 | Если используется аутентификация без сохранения состояния(stateless), сервер предоставляет токен, подписанный с использованием безопасного криптоалгоритма. Долны выполняться базовые требования к работе с токенами. | Для Android: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing- Platform-Interaction.md Для iOS: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md |
|  | SM13 | Бэкенд удаляет существующую сессию, когда пользователь выходит из системы |  |
|  | SM1 | Session IDs, передающиеся с помощью cookies должны настроены с использованием флагов безопасности(http only, secure, path) | Для тестирования корректности параметров Cookies можно использовать любые решения для перехвата https трафика. Необходимо запустить инструмент после чего пройти процедуру аутентифкации в тестируемом приложении. Все передаваемые пакеты, в том числе содержащие Cookies можно будет просмотреть в интерфейсе используемого инструмента и проверить корректность значений для параметров http only, secure, path  Примеры инструментов для проведения проверки: Intercepting Proxy OWASP Zed Attack Proxy Project Web Proxy Burp Suite  Плагины для браузеров: EditThisCookie for Chrome |
|  | SM2 | Session ID должен быть сменен при аутентификации, повторной аутентификации или смене привилегий учетной записи. | Для тестирования корректности параметров Cookies можно использовать любые решения для перехвата https трафика.  1.Необходимо запустить инструмент 2. Зайти на страницу аутентификации тестируемого приложения и посмотреть текущий Session ID  3. Пройти процедуру аутентифкации в тестируемом приложении. Проверить в инструменте, что Session ID был изменен 4. Зайти в систему с правами администратора и изменить пользователю полномочия в системе. Убедиться, что также произошло изменение Session ID.  Примеры инструментов для проведения проверки: Intercepting Proxy OWASP Zed Attack Proxy Project Web Proxy Burp Suite |
|  | SM3 | Функциональность по принудительному завершению сессии пользователем(Logout) должна быть доступна на каждой странице приложения | 1. При использовании доменной аутентификации в АС требование не проверяется (выполняется на уровне домена). 2. Войти в АС с правами любого пользователя. Нажать на кнопку принудительного заврешения сессии. 3. Попытаться выполнить любое действие в АС. Убедиться в том, что никакое действие в АС выполнить невозможно, кроме ввода логина и пароля для повторного входа в АС. |
|  | SM4 | В приложении должен быть реализован настраиваемый механизм конфигурирования абсолютного времени жизни сессий пользователей | 1. Войти в АС с правами админитартора ИБ. Проверить установленное значение времени сессии. 2. Убедиться в том, что его значение соответствует указанному в Корпоративном стандарте  3. Войти в АС с правами прикладного администратора.  4. Установить время сессии пользователя 30 – 60 секунд. Выйти из АС.  5. Войти в АС с правами любого пользователя. Не выполняя никаких действий, выждать установленное время.  6. Попытаться выполнить любое действие в АС. Убедиться в том, что никакое действие в АС выполнить невозможно, кроме ввода логина и пароля для входа в АС. Ввести корректные логин пароль и войти в АС.   Критичные ошибки:  1. Невозможность установки времени жизни сессии пользователя. 2. АС позволяет пользователю выполнить какое-либо действие кроме ввода логина и пароля для входа в АС после истечения установленного времени |
|  | SM5 | В приложении должен быть реализован настраиваемый механизм конфигурирования времени жизни сессий пользователей в случае неактивности | 1. Проверить описание способа аутентификации в Архитектурной документации на АС 2. При использовании доменной аутентификации в АС требование не проверяется (выполняется на уровне домена). 3. При использовании локальной аутентификации проверить наличие описания процесса установки времени бездействия в Руководстве администратора АС. 4. Войти в АС с правами админитартора ИБ. Проверить установленное значение времени бездействия. Убедиться в том, что его значение соответствует указанному в Корпоративном стандарте 5. Войти в АС с правами прикладного администратора. 6. Установить время бездействия пользователя 30 – 60 секунд. Выйти из АС. 7. Войти в АС с правами любого пользователя. Не выполняя никаких действий, выждать установленное время. 8. Попытаться выполнить любое действие в АС. Убедиться в том, что никакое действие в АС выполнить невозможно, кроме ввода логина и пароля для входа в АС. Ввести корректные логин пароль и войти в АС.    Критичные ошибки:  1. Невозможность установки времени бездействия пользователя. 2. АС позволяет пользователю выполнить какое-либо действие кроме ввода логина и пароля для входа в АС после истечения установленного времени бездействия или блокировки сеанса доступа пользователя по запросу администратора АС. |
|  | SM6 | Session ID должен быть связана с параметрами подключения пользователя (например с user agent / типом устройства/данными геолокации) |  |
|  | SM7 | Параметр, определяющий количество конкурентных сессий для одного пользователя должен быть настраиваемым на стороне приложения | 1. Проверить в документации на АС описание возможности осуществления параллельных сеансов доступа и настройки ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя АС (на технические учетные записи данное ограничение не распространяется). 2. В соответствии с документацией осуществить вход в АС под УЗ пользователя. Выполнить какое-либо дополнительное отражаемое в журнале аудита действие. 3. Осуществить вход в АС под УЗ того же пользователя с другого рабочей станци. Выполнить какое-либо дополнительное отражаемое в журнале аудита действие. 4. Выйти из АС. Войти в АС под УЗ Администратора ИБ. Осуществить просмотр журнала аудита. 5. Убедиться в том, что в журнале аудита присутствуют записи о двух событиях успешного входа в АС пользователя и о двух выполненных дополнительных действиях, и что в каждой из этих четырех записей присутствуют признаки, разделяющие сеансы доступа и позволяющие объединить события одного сеанса, отличить события одного сеанса от другого. 6. В настройках АС установить для УЗ одного из пользователей блокировку возможнсоти одновременных сеансов с разных устройств. 7. Под УЗ этого пользователя выполнить действия, описанные в п. 2-3 8. Осуществить попытку входа в АС того же пользователя с новой рабочей станции. 9. Убедиться в том, что вход в АС под УЗ данного пользователя со второй рабочей станции невозможен.  Критичные ошибки: 1. В журнале аудита отсутствуют записи о соответствующих событиях входа пользователя  2. Вход в АС под УЗ пользователя со второй рабочей станции после установки ограничения оказался успешным. |
|  | SM8 | Пользователю должна быть предоставлена возможность просмотра и завершения всех активных сессий |  |
|  | SM9 | Необходимо ограничивать максимальное количество одновременных запросов к серверу |  |
|  | SM10 | В случае отсутствия в приложении механизма управления жизненным циклом токенов в приложении должны поддерживать чёрные списки JWT-токенов |  |
|  | **AU** | **Технические. Идентификация и аутентификация** |  |
|  | AU14 | Для выполнения критичных операций в приложении(регистрация и восстановление аккаунта) не должен использоваться небезопасные каналы взаимодействия (e-mail или колл-центр). |  |
|  | AU10 | Подтверждение финансовых операций должно осуществляться с использованием одноразовых паролей |  |
|  | AU1 | Все интерфейсы и ресурсы приложения должны быть доступны только после успешного прохождения аутентификации |  |
|  | AU2 | В качестве Single Sign-On провайдера может быть использован только корпоративный каталог пользователей |  |
|  | AU13 | Приложение информирует пользователей о всех важных действиях с их учетной записью. Пользователи могут просматривать список устройств, просматривать дополнительную информацию (IP-адрес, местоположение и т.д.), и блокировать конкретные устройства. |  |
|  | AU12 | В приложении реализована и применяется двухфакторная аутентификация. Второй фактор может использоваться только на этапе выполнения критичных функций в приложении. |  |
|  | AU3 | В приложении должны быть реализованы механизмы, позволяющие противодействовать атакам, связанным с перебором паролей пользователей |  |
|  | AU4 | Перед проведением критичных с точки зрения безопасности операций(например, смены пароля, проведение финанисовой операции, изменения способа аутентификации) должна осуществляться повторная аутентификация пользователей |  |
|  | AU5 | В приложении должен быть реализован настраиваемый механизм конфигурирования параметров сложности паролей пользователей |  |
|  | AU6 | В приложении должен быть реализован настраиваемый механизм конфигурирования времени жизни паролей пользователей | Improper Authorization in Handler for Custom URL Scheme - https://cwe.mitre.org/data/definitions/939.html  Для Android: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing- Platform-Interaction.md Для iOS: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md |
|  | AU7 | Должно осуществляться уведомление пользователя в случае выявления попыток входа в приложения(как успешных, так и не успешных) из необычного окружения |  |
|  | AU8 | Должно осуществляться уведомление пользователя в случае смены его пароля в приложении | Методика проверки SM5 |
|  | AU9 | Процедура восстановления забытого пароля не должна отличаться по стойкости от процедуры его первичного получения |  |
|  | **AC** | **Технические. Разграничение доступа** |  |
|  | AC1 | Механизмы разграничения доступа должны быть реализованы на стороне сервера и использовать только надежные реализации |  |
|  | AC2 | Разграничение доступа должно быть реализовано в соответсвии с матрицей ролей |  |
|  | AC3 | Пользователям должны быть предоставлены только минимально необходимые полномочия, необходимые для реализации бизнес-процесса. |  |
|  | AC4 | В приложение должны быть настроены лимиты на выполняемые операций и функций(максимальное количество просмотров карточек клиентов в час, количество отправляемых по почте уведомлений в день и т.д.) |  |
|  | AC5 | Для запуска Node.js не должен использоваться пользователь, обладающий root-привилегиями |  |
|  | **IV** | **Технические. Валидация входных данных** |  |
|  | IV4 | Должны быть реализованы механизмы противодействия атакам типа Cross-Site Request Forgery |  |
|  | IV1 | Для валидации данных должен использоваться только согласованный и проверенный на предмет соответствия требованиям по безопасности набор библиотек |  |
|  | IV2 | Конфиденциальная информация никогда не должна передаваться методом GET |  |
|  | IV3 | Параметры валидации должны в явном виде определять допустимые значения для данных. Все, не советующие правилам данные не должны обрабатываться в приложении. |  |
|  | IV5 | Должны быть реализованы механизмы противодействия атакам типа Clickjacking |  |
|  | IV6 | Редиректы не должны содержать не проверенных данных |  |
|  | IV7 | В случае реализации в приложении функциональности по загрузке файлов необходимо осуществлять валидацию контента, включая проверку на наличие во вложении вредоносного кода |  |
|  | IV8 | Должны быть реализованы механизмы противодействия атакам типа переполнение буффера( Buffer overflow) |  |
|  | IV9 | В случае если для работы приложения обязательно использование небезопасного кода его выполнение должно осуществляться в песочнице |  |
|  | **OE** | **Технические. Валидация вывода** |  |
|  | OE1 | Для валидации данных, передаваемых в любые интерфейсы должен использоваться только согласованный и проверенный на предмет соответствия требованиям по безопасности набор практик |  |
|  | OE2 | Неэкранированные данные не должны передаваться в HTTP заголовки |  |
|  | OE3 | Неэкранированные данные не должны записываться в журналы аудита |  |
|  | OE4 | Неэкранированные данные не должны передаваться в качестве параметров для системных команд операционной системы |  |
|  | **CR** | **Технические. Криптография и генерация случайных чисел** |  |
|  | CR10 | При реализации взаимной аутентификации с помощью сертификатов приложение верифицирует серверные X.509 сертификаты во время установления защищённого соединения. Принимаются только сертификаты, подписанные доверенными удостоверяющими центрами |  |
|  | CR9 | Данные, передаваемые по сети от клиентской части к приложения до бэкэнда шифруются с использованием протокола TLS |  |
|  | CR8 | Приложение не переиспользует один и тот же ключ для различных целей |  |
|  | CR7 | В приложение не используются устаревшие и слабые криптографические протоколы и алгоритмы. |  |
|  | CR1 | Криптографические библиотеки должны применяться в приложении для достижения описаных в документации целей и должны быть настроены в соответствии с задокументированными требованиями по безопасности |  |
|  | CR2 | Применение средств криптографической защиты должно осуществляться с учетом утвержденной политики по управлению ключевой информацией |  |
|  | CR3 | Для хранения паролей в приложении должно использоваться хэширование с солью |  |
|  | CR4 | Для генерации случайных чисел должен использоваться согласованный и проверенный на предмет соответствия требованиям по безопасности набор методов |  |
|  | CR5 | Для обработки паролей не должен использоваться стандартный модуль Node.js crypto. Вместо него необходимо применять Bcrypt |  |
|  | **EH** | **Технические. Обработка ошибок** |  |
|  | EH3 | Логика обработки ошибок, связанных с реализаций функций безопасности по-умолчанию должна предполагать блокирование доступа. |  |
|  | EH1 | В случае возникновения ошибок в работе приложения, содержащаяся в описании ошибки информация не должна содержать чувствительных данных, которые могут быть использованы злоумышленником |  |
|  | EH2 | Файл Robots.txt не должен содержать чувствительной информации |  |
|  | **LO** | **Технические. Журналирование** |  |
|  | LO1 | Все имеющие отношение к информационной безопасности и описанные в документации параметры должны журналироваться при изменении. |  |
|  | LO2 | Все имеющие отношение к безопасности события, содержащиеся в журналах аудита должны содержать всю необходимую информацию для их интерпретации |  |
|  | LO3 | В приложении не должны журналироваться данные, которые могут помочь злоумышленнику для реализации атаки (например: идентификаторы клиентских сессий, коды, персональные данные, отладочные сообщения и т.д). Отладочный код и скрытые настройки удалены из приложения. |  |
|  | **DP** | **Технические. Защита данных** |  |
|  | DP6 | Конфиденциальные данные не должны передаваться третьей стороне, кроме случаев если это часть бизнес функциональности приложения |  |
|  | DP10 | Конфиденциальные данные не сохраняются в бэкапы, создаваемые операционной системой |  |
|  | DP1 | Чувствительная информация, сохраненная в кэше системы должна быть защищена от неавторизованного доступа и очищена сразу же после достижения целей обработки | Данное требование не требуется проверять технически |
|  | DP2 | Пароли, используемые для подключения к компонентам приложения и другим приложениям не должны храниться в открытом виде |  |
|  | DP8 | Чувствительные данные недоступны через механизмы межпроцессного взаимодействия (IPC). |  |
|  | DP5 | Для хранения чувствительных данных, таких как персональные данные, аутентификационная информация и криптографические ключи должно использоваться хранилище для конфиденциальной информации предоставляемое платформой(Android, iOS). |  |
|  | DP12 | Приложение хранит чувствительные данные в памяти только на время необходимое для обработки и полностью удаляет их из памяти после завершения работы с ними. |  |
|  | DP3 | Пароли никогда не должны храниться в клиентской части приложения |  |
|  | DP4 | Чувствительные данные передаваемые клиентской части приложения должны быть защищены от кэширования за счет использования соответствующих HTTP заголовков |  |
|  | **CS** | **Технические. Безопасность подключений** |  |
|  | CS1 | Передача информации между компонентами приложения и другими приложениями должна осуществляться только по защищенным протоколам | Необходимо убедиться, что: - обфусцированы все значимые идентификаторы, такие как имена классов и методов, а также имена переменны; - строковые ресурсы и переменные в бинарном коде зашифрованы;  - данные, относящиеся к критичной функциональности приложения зашифрованы или скрыты иным образом |
|  | CS2 | В приложении должна быть реализована Content Security Policy |  |
|  | CS3 | Для обеспечения безопасности приложения должны быть корректно настроены относящиеся к безопасности HTTP заголовки |  |
|  | **CO** | **Технические. Общие требования и документирование** |  |
|  | CO1 | В документации на приложения должны быть перечислены все используемые криптографические библиотеки, цели и способы их применения, а так же их настройки по безопасности |  |
|  | CO2 | В документации на приложение должны быть перечислены все имеющие отношение к информационной безопасности параметры |  |
|  | **CQ** | **Технические. Качество кода и безопасность сборки** |  |
|  | CQ5 | Используются все стандартные функции безопасности, предоставляемые инструментами для разработки (такие как обфускация, минификация байт-кода, защита стека, поддержка PIE и ARC). |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверки проводятся в соответствии с методикой, изложенной в настоящем документе. В случае выявления при проверке ошибок или несоответствий по решению тестировщика от Блока ИБ могут быть проведены дополнительные тесты с целью уточнения степени соответствия АС требованиям по ИБ.