АКЦИОНЕРНОЕ ОБЩЕСТВО

ПРИКАЗ

16.01.2020 № 7-п

МОСКВА

[Об утверждении Стандарта «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений АО «Почта России»]

В соответствии с графиком пересмотра, а также для обеспечения конфиденциальности, целостности и доступности обрабатываемой АО «Почта России» информации п р и к а з ы в а ю:

1. Утвердить прилагаемый Стандарт «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений АО «Почта России».

2. Признать утратившим силу Стандарт «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений ФГУП «Почта России», утвержденный 23.11.2016 № 1.9.3.1.2-05/98-нд.

Заместитель генерального директора
по информационным технологиям
и развитию цифровых сервисов С.Е. Емельченков

Приложение

УТВЕРЖДЕНО
приказом АО «Почта России»
от 16.01.2020 № 7-п

СТАНДАРТ
«Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений АО «Почта России»

Москва, 2020

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Стандарте «Обеспечение информационной безопасности при разработке или модернизации информационных систем или приложений АО «Почта России» (далее – Стандарт) используются следующие термины и определения.

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Авторизация		Процедура проверки прав доступа перед выполнением какого-либо действия.
Аутентификационная информация		Информация, используемая для подтверждения наличия прав доступа (идентификатор, пароль, отпечаток пальца или др.).
Аутентификация		Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).
Внешний интерфейс		Сервис, через который осуществляется непосредственное взаимодействие с внешними пользователями или информационными системами (web-страница или API).
Внутренний интерфейс		Сервис, через который осуществляется непосредственное взаимодействие с внутренними пользователями или информационными системами.
Департамент информационной безопасности	ДИБ	Департамент информационной безопасности Блока по корпоративной безопасности.
Информационная безопасность	ИБ	Состояние защищенности информации (данных) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации, и характеризуемое способностью обеспечивать конфиденциальность, целостность и доступность информации при ее хранении, обработке и передаче на заданном владельцем уровне.
Информационная система	ИС	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информационная система персональных данных	ИСПДн	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Информация ограниченного доступа		Информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Коммерческая тайна	КТ	Информация, доступ к которой ограничивается на основании нормативных документов Общества.

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Компонент системы		Любое сетевое устройство, сервер или приложение, входящее в состав ИС или подключенное к среде передачи данных.
Конфиденциальная информация (информация конфиденциального характера)	КИ	Информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и информация, доступ к которой ограничивается на основании нормативных документов Общества.
Минимально необходимые права доступа		Набор прав доступа в ИС, позволяющие выполнять в ней операции, определяемые должностными обязанностями работника, и не превышающие их.
Модель угроз		Документ, в котором определяются актуальные для Системы угрозы ИБ.
Модернизация системы		Полное или частичное изменение системы или ее компонентов, в том числе изменение исходного кода, установка обновлений и дополнительных модулей, настройка взаимосвязей.
Обработка данных		Сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение данных.
Обфускация		Приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.
Общество		АО «Почта России».
Операционная Система	ОС	Комплекс программ, обеспечивающий управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных задач и утилит.
Персональные данные	ПДн	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Пользователь		Лицо, участвующее в функционировании ИС.
Права доступа пользователя		Совокупность правил, регламентирующих порядок и условия доступа пользователя к информации и ее носителям, установленных нормативными документами или владельцем информационного актива (ресурса).
Сегмент сети		Логически или физически обособленная часть сети.
Система		См. «**Информационная система**».
Система управления базами данных	СУБД	Совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Технические документы		Документы, описывающие техническую часть системы, а именно: техническое задание, частное техническое задание, технический проект, частный технический проект, целевая архитектура и другие.
Угроза информационной безопасности		Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информационным активам, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий при их обработке в ИС.
Active Directory	AD	Инфраструктурная информационная система, предназначенная для обнаружения и управления сетевыми ресурсами компании (ученые записи пользователей, группы, принтеры, компьютеры и т.п.).
Application programming interface	API	Программный интерфейс-приложения, с помощью которого одна компьютерная программа может взаимодействовать с другой программой.
Completely Automated Public Turing test to tell Computers and Humans Apart	CAPTCHA	Компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером.
Cookies		Небольшой фрагмент данных, отправленный web-сервером и хранимый на компьютере пользователя.
Demilitarized zone	DMZ	Отдельный сегмент сети, изолированный от основных сегментов сети с помощью межсетевого экрана. Предназначен для размещения ресурсов, к которым возможен доступ из сети Интернет.
Domain Name System	DNS	Служба доменных имен. Представляет собой распределенную, иерархическую базу данных для хранения имен сетей и компьютеров. Также предоставляет функционал по преобразованию строчных имен в числовые IP-адреса.
Fully Qualified Domain Name	FQDN	Точное обозначение имени оборудования в рамках службы DNS.
File Transfer Protocol	FTP	Протокол для передачи данных. Обеспечивает передачу данных из файловой системы сервера в локальную файловую систему клиента и наоборот.
File Transfer Protocol over SSL	FTPS	Дополнение к протоколу FTP, позволяющее передавать его данные поверх протокола TLS/SSL.

Наименование термина	Сокраще-ние	Определение термина (расшифровка сокращения)
Identity Manager	IDM	Централизованная система, используемая для управления данными пользователей и для синхронизации между несколькими основными пользовательскими хранилищами информации, которые используются для хранения параметров и идентификационной информации.
Network Time Protocol	NTP	Протокол сетевого времени. Протокол, с помощью которого производится синхронизация системного времени компьютера с временем NTP-сервера.
Secure copy	SCP	Протокол копирования файлов, использующий в качестве транспорта протокол SSH.
Secure Multipurpose Internet Mail Extensions	S/MIME	Набор стандартов описывающих безопасную передачу различных типов данных посредством электронной почты и других средств.
SSH File Transfer Protocol	SFTP	Протокол, предназначенный для обмена и управления данными поверх какого-либо криптографического протокола (обычно SSH).
Structured Query Language	SQL	Структурированный язык запросов. Специализированный информационно-логический язык, используемый для работы с данными в реляционных СУБД.
Secure Shell	SSH	Протокол, позволяющий передавать данные и производить удаленное управление операционной системой по защищенному каналу.
Transport Layer Security	TLS	Криптографический протокол, обеспечивающий конфиденциальность и целостность данных при их передаче по сети.
Uniform Resource Locator	URL	Универсальный указатель ресурса.
Virtual Local Area Network	VLAN	Логическое разделение компьютерной сети на канальном уровне.
Virtual Private Network	VPN	Виртуальная частная сеть. Логическая сеть, создаваемая поверх другой сети, и использующаяся для безопасной пересылки данных.
Web-приложение		Клиент-серверная Система, в которой клиентом выступает браузер, а сервером – web-сервер.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящий Стандарт разработан с целью унификации требований по ИБ, предъявляемых к новым или модернизируемым Системам и приложениям Общества, обеспечения конфиденциальности, целостности и доступности обрабатываемой в них информации с учетом исполнения требований

законодательства Российской Федерации, семейства стандартов ISO/IEC 27000, локальных нормативных документов Общества.

Требования настоящего Стандарта распространяются на все подразделения Общества, осуществляющие деятельность по разработке, модернизации и эксплуатации ИС и приложений.

Подразделением, ответственным за координацию и контроль исполнения настоящего Стандарта является ДИБ.

Отступление от требований настоящего Стандарта осуществляется по согласованию с ДИБ.

Настоящий Стандарт подлежит пересмотру и актуализации (в случае необходимости) не реже одного раза в три года, а также в случае изменений законодательства в области ИБ, касающихся положений данного Стандарта.

Актуальная версия Стандарта размещается на корпоративном портале или может быть предоставлена по электронной почте по соответствующему запросу в ДИБ.

3. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

3.1. Работы по обеспечению ИБ должны проводиться на всех этапах жизненного цикла ИС.

3.2. Работники ДИБ должны включаться в состав комиссии (проектной команды) по разработке или модернизации ИС.

3.3. Требования настоящего Стандарта должны в обязательном порядке включаться в технические документы на разработку или модернизацию ИС (технические задания, частные технические задания, технические проекты, частные технические проекты, целевые архитектуры и другие).

3.4. Объем требований по обеспечению ИБ, включаемый в технические документы, определяется в рамках процесса его согласования с ДИБ. Исключение требований данного Стандарта из технических документов возможно с учетом обоснования такой потребности и ее согласования с ДИБ.

3.5. В рамках работ по созданию или модернизации Системы ДИБ должен провести ее испытания по проверке исполнения требований настоящего Стандарта, а также отсутствия уязвимостей Системы.

3.6. Ввод Системы в эксплуатацию (опытную / промышленную) возможен после успешного прохождения испытаний Системы и получения положительного заключения о ее соответствии требованиям ИБ.

4. ТРЕБОВАНИЯ К РАЗРАБАТЫВАЕМЫМ ИЛИ МОДЕРНИЗИРУЕМЫМ СИСТЕМАМ

4.1. Общие требования

4.1.1. КИ, обрабатываемая внутри корпоративной сети, должна быть защищена с использованием криптографически стойких алгоритмов шифрования.

Перечень криптографически стойких алгоритмов (Приложение № 1 к Стандарту) размещается на корпоративном портале совместно с настоящим

Стандартом и может быть предоставлен ДИБ по электронной почте по запросу.

4.1.2. Данные, содержащие персональные данные, информацию, обрабатываемую в государственных информационных системах, и иную информацию, обеспечение конфиденциальности которой определяется законодательством Российской Федерации, при передаче по сетям общего пользования должны защищаться с использованием средств криптографической защиты информации, имеющих сертификат соответствия ФСБ России.

4.1.3. Система и ее компоненты, расположенные в DMZ, не должны хранить информацию конфиденциального характера Общества.

4.1.4. Тестовые и учебные экземпляры Системы не должны содержать реальных данных конфиденциального характера либо должны содержать их в обезличенном виде.

4.1.5. Внешние интерфейсы Системы, предоставляющие доступ из общедоступных сетей клиентам Общества, и внутренние интерфейсы Систем, предназначенные для использования администраторами и внутренними привилегированными пользователями, должны быть разделены.

4.1.6. Возможность управления сервисами безопасности, в том числе отключения, подключения, модификации режима аутентификации, авторизации, аудита и т.п., должна быть доступна только администратору Системы.

4.1.7. Проверка входных данных

4.1.7.1. Должна осуществляться проверка любых входных данных на стороне сервера на длину, допустимые символы, кодировку, полноту данных (наличие обязательных параметров).

4.1.7.2. Рекомендуется корректировать данные перед передачей на сторону сервера (удаление лишних символов, приведение к единому формату и т.п.).

4.2. Требования к аутентификации и авторизации

4.2.1. Доступ к ресурсам Системы должен предоставляться только после успешного прохождения процесса аутентификации пользователя и последующей его авторизации.

4.2.2. Доступ к ресурсам Системы должен подразделяется на пользовательский, административный, технологический и должен быть реализован на основе ролей с учетом принципов разделения обязанностей и минимизации полномочий. В Системе необходимо наличие средств управления ролями: создание новых, редактирование, удаление.

4.2.3. Управление доступом к Системе должно осуществляться на основании групповой или ролевой моделей: функции и данные в Системе должны быть разбиты на группы, связанные с ролями пользователей.

4.2.4. Внешние и внутренние пользователи должны проходить аутентификацию во внешней и внутренней системе аутентификации

соответственно. Внешняя и внутренняя системы аутентификации должны быть разделены.

4.2.5. Внутренняя система аутентификации должна интегрироваться с системой AD Общества или корпоративной IDM.

4.2.6. Для каждого пользователя необходимо использовать следующие основные атрибуты безопасности: идентификатор пользователя, аутентификационная информация (например, пароль), права доступа к объекту защиты (роль).

4.2.7. Для каждого пользователя необходимо использовать уникальную учетную запись, сформированную в соответствии с принятыми в Общества правилами именования.

4.2.8. Использование групповых учетных записей запрещено.

4.2.9. В Системе и ее компонентах должны отсутствовать жестко запрограммированные учетные записи.

4.2.10. Все неиспользуемые учетные записи (установленные по умолчанию, тестовые, сервисные) для штатной работы Системы и ее компонентов должны быть удалены или заблокированы.

4.2.11. В качестве механизмов аутентификации пользователей Системы могут быть использованы:

– аутентификация на основе паролей (пароль, пин-код или др.);

– аутентификация на основе одноразовых паролей (sms, генераторы одноразовых паролей и др.);

– аутентификация при помощи хранилища ключей (USB-токен, смарт-карта и т.п.);

– средства биометрической аутентификации.

4.2.12. Для ИС, обрабатывающих КИ, рекомендуется использование второго фактора аутентификации.

4.2.13. Для подтверждения критичных действий в Системе (к примеру, выполнение финансовых операций) рекомендуется повторная аутентификация или аутентификация с помощью второго фактора.

4.2.14. В процессе аутентификации проверка учетных данных должна осуществляться только после полного их ввода.

4.2.15. В случае обнаружения ошибки при аутентификации Система не должна уточнять, какие именно данные введены неправильно.

4.2.16. Проверка учетных данных должна проводиться на стороне серверных компонентов Системы.

4.2.17. Механизмы авторизации пользователей Системы должны поддерживать возможность разделения доступа к данным и функциям внутри Системы.

4.2.18. Все действия в Системе, включая администрирование и штатную эксплуатацию, должны производиться с использованием учетных записей, наделенных минимально необходимыми привилегиями.

4.2.19. Компоненты Системы с повышенными требованиями к обеспечению ИБ в случае сетевого взаимодействия, например, при передаче

по сети финансовых операций, должны проходить процедуру взаимной аутентификации.

4.2.20. Процесс аутентификации и авторизации должен быть устойчив к сетевым угрозам (пассивному и активному прослушиванию сети, подбору паролей и т.п.).

4.2.21. До авторизации Система должна предоставлять пользователю минимальные необходимые данные о себе (к примеру, данные, которые могут потребоваться для решения проблем со входом в Систему).

4.2.22. Пароль не должен отображаться при вводе.

4.2.23. Соответствие требованиям парольной политики.

Подсистема аутентификации Системы должна соответствовать требованиям документа «Частная политика информационной безопасности. Парольная политика», в том числе:

4.2.23.1. Настроена обязательная смена пароля пользователем при первом входе в Систему.

4.2.23.2. Настроена возможность смены пароля пользователем, но не чаще одного раза за определенный период времени (рекомендуется раз в сутки).

4.2.23.3. У администратора имеется возможность отключения функции смены паролей у отдельных учетных записей.

4.2.23.4. Реализована возможность установки отдельной парольной политики для всех пользователей, для группы пользователей или отдельно для каждой учетной записи в соответствии с локальными нормативными документами Общества.

4.2.23.5. Восстановление пароля должно производиться только путем его смены.

4.2.23.6. Настроена принудительная смена пароля пользователем через установленный промежуток времени.

4.2.23.7. Реализовано заблаговременное оповещение пользователей о необходимости смены пароля (посредством сообщений / подсказок или почтовых рассылок на электронные адреса пользователей).

4.2.23.8. Настроена блокировка учетной записи на заранее определенный срок после заданного количества неудачных попыток аутентификации.

4.2.23.9. Установлена длительность простоя пользовательской сессии, после которой сессия должна принудительно блокироваться.

4.2.23.10. Ограничен множественный вход в Систему под одной учетной записью пользователя.

4.2.23.11. Реализовано хранение и передача паролей только в зашифрованном виде. При хранении и передаче должны использоваться стойкие криптографические алгоритмы или алгоритмы хеширования, определенные в соответствии с пунктом 4.1.1.

Дополнительно для внутренних пользователей подсистема аутентификации Системы должна осуществлять:

4.2.23.12. Настроена автоматическая блокировка входа в Систему с учетной записью пользователя в случае, если пароль не был изменен до установленной даты.

4.2.23.13. Реализовано хранение истории паролей пользователей не менее чем за последние 12 месяцев для предотвращения повторного их использования.

4.3. Требования к сетевому взаимодействию

4.3.1. Сетевой обмен информацией между компонентами Системы, сопрягаемыми Системами, находящимися в разных сетевых сегментах, должен осуществляться с использованием защищенных стандартов и протоколов, таких как:

- HTTPS/TLS;
- SFTP;
- FTPS;
- SSH-2;
- SCP;
- S/MIME с использованием сертификатов x.509 v3;
- VPN (IPSEC, L2TP, PPTP и т.д.).

4.3.2. DNS-имена внешних / внутренних компонентов Системы (FQDN) должны быть зарегистрированы соответственно в прямой и обратной зонах внешних / внутренних служб DNS Общества.

4.3.3. Сетевое взаимодействие Системы и ее компонентов должно производиться с использованием FQDN, если это технически возможно.

4.3.4. Ни один из серверов Системы не должен подключаться одновременно к сетевым периметрам с различными уровнями безопасности (например, DMZ и корпоративная сеть).

4.3.5. Доступ к компонентам Системы, размещенным в DMZ, должен осуществляться с использованием минимально необходимого набора сетевых протоколов и FQDN.

4.3.6. Серверные компоненты Системы должны размещаться в серверных сегментах сети Общества.

4.3.7. Продуктивная среда Системы должна быть разделена со средой разработки, тестовой средой и беспроводным сегментом на физическом / виртуальном и логическом уровне. Например, тестовая среда Системы должна представлять собой отдельную копию Системы, не взаимодействующую с какими-либо продуктивными средами Систем.

4.3.8. При взаимодействии с сетью Интернет должны выполняться следующие требования:

4.3.8.1. Доступ из сети Интернет разрешен только к компонентам Системы, относящимся к продуктивной среде и расположенным в DMZ.

4.3.8.2. Для организации защищенного удаленного доступа к ресурсам Системы возможно использование централизованного VPN-шлюза Общества. Использование самостоятельных решений для удаленного доступа недопустимо.

4.3.8.3. Запрещен доступ из сети Интернет к сервисам Системы, предназначенным для внутреннего использования.

4.3.8.4. Запрещен доступ из сети Интернет к сервисам Системы, использующим для взаимодействия с пользователями следующие протоколы: SMB/SAMBA/CIFS, NFS, NETBIOS, протоколы доступа к СУБД (MYSQL, MSSQL, ORACLE и др.), протоколы удаленного управления (telnet, SSH, RSH, SNMP, RDP и др.).

4.3.8.5. Внешние (публичные) интерфейсы Системы должны быть размещены в DMZ.

Предоставление доступа из сети Интернет возможно только после проведения ДИБ аудита ИБ (см. п.4.7.1).

4.3.8.6. Запрещено использование облачных Интернет-сервисов хранения данных в качестве компонентов Системы. Требование не распространяется на частные облачные ресурсы, размещенные в пределах сети Общества.

4.4. Требования к окружению

4.4.1. Система должна корректно функционировать с используемыми в Обществе средствами обеспечения безопасности рабочих станций и серверов, например, антивирусами, средствами обнаружения и предотвращения вторжений, средствами межсетевого экранирования, средствами контроля внешних устройств, средствами криптографической защиты информации и т.д.

Перечень средств обеспечения безопасности рабочих станций и серверов, используемых в Обществе и с которыми должна быть совместима разрабатываемая или модернизируемая Система, должен уточняться и согласовываться с ДИБ в рамках предпроектного обследования.

4.4.2. Система должна корректно функционировать с используемыми в Обществе ОС, СУБД, прикладными программами с действующими на момент разработки или модернизации Системы настройками.

4.4.3. Разрабатываемые компоненты Системы, включая программное и аппаратное обеспечение, не должны содержать недокументированных возможностей, направленных на скрытый контроль пользователей или скрытый контроль администраторов Системы (например, отправка информации в сеть Интернет о действиях в Системе).

4.4.4. На компонентах Системы должны быть запущены только те сервисы и приложения, которые необходимы для функционирования данной Системы или функционирования других Систем (при совместном использовании компонент).

4.4.5. Взаимодействие компонент Системы, а также взаимодействие с внешними Системами должно происходить под технологическими учетными записями с минимально необходимыми наборами привилегий.

4.4.6. Компоненты Системы должны быть построены исключительно на продуктах и ОС, удовлетворяющих всем требованиям безопасности

настоящего Стандарта, а также стандартов ИБ Общества, разработанных для конкретных ОС, СУБД и приложений.

Стандарты ИБ для конкретных ОС, СУБД и приложений утверждаются заместителем генерального директора по корпоративной безопасности Общества, размещаются на корпоративном портале совместно с настоящим Стандартом и могут быть предоставлены ДИБ по электронной почте по запросу.

4.5. Требования к аудиту

4.5.1. Для Системы и ее компонент (включая уровни ОС, СУБД и Приложения) должен быть включен механизм протоколирования событий.

4.5.2. Механизм протоколирования событий должен быть способен сопоставить каждое подлежащее аудиту событие с источником события с возможным определением IP адреса источника.

4.5.3. Время, указываемое в журналах аудита, должно быть синхронизировано с системным временем корпоративного NTP-сервера, являющегося частью инфраструктуры сети Общества (допустимая погрешность не более 5 секунд).

4.5.4. Система должна предоставлять средства фильтрации событий журнала аудита по протоколируемым параметрам.

4.5.5. Система должна поддерживать сохранение журналов аудита в систему сбора и хранения логов ИС Общества. При этом могут быть использованы следующие способы доступа к журналам аудита: сетевой доступ к файлу с журналом, SQL доступ к таблице с журналом, SNMP, Syslog, Eventlog и т.д.

4.5.6. Журналы аудита Системы не должны содержать данных конфиденциального характера (например, пароли пользователей).

4.5.7. Журналы аудита Системы должны быть защищены от изменений.

4.5.8. Сроки хранения журналов аудита

4.5.8.1. Срок хранения журналов аудита в оперативном доступе в Системе должен составлять не менее трех месяцев.

4.5.8.2. По истечении установленного времени хранения журналов аудита в оперативном доступе они должны автоматически архивироваться.

4.5.8.3. Срок хранения журналов аудита в архивном доступе должен составлять не менее одного года, после чего они могут быть удалены.

4.5.8.4. Журналы аудита должны иметь возможность автоматического разбиения и хранения по месяцам.

4.5.9. В Системе как минимум должны протоколироваться следующие события:

4.5.9.1. Работа пользователей с данными Системы, в том числе создание, чтение, изменение или удаление данных.

4.5.9.2. События аутентификации пользователя в Системе (включая неуспешные), выход (окончание сессии) из Системы, если технически применимо.

4.5.9.3. Действия привилегированных пользователей по настройке и изменению конфигурации Системы, в том числе изменение настроек Системы, настроек аудита, создание / удаление пользователей / ролей / групп пользователей, изменение привилегий пользователей / ролей / групп пользователей, установка / удаление компонент Системы.

4.5.9.4. Доступ к записям журнала протоколирования событий.

4.5.9.5. Очистка логов.

4.5.9.6. Запуск и остановка компонентов Системы.

4.5.10. По каждой операции должна протоколироваться следующая информация:

4.5.10.1. Результат операции (успешно / неуспешно).

4.5.10.2. Идентификатор источника операции (идентификатор пользователя, логин пользователя, имя процесса, IP-адрес, идентификатор рабочей станции и т.д.).

4.5.10.3. Идентификатор объекта, над которым была выполнена операция.

4.5.10.4. Название и тип выполненной операции (например, аутентификация, чтение, запись, удаление, установление соединения и др.).

4.5.10.5. Значение параметра до и после операции, если действие предполагает изменение данных или состояния компонента Системы.

4.5.10.6. Дата и время выполнения операции, включая указание часового пояса.

4.6. Требования по отказоустойчивости

4.6.1. Система должна разрабатываться с учетом возможности балансирования нагрузки между отдельными компонентами и модулями. При этом выход из строя отдельных компонент или модулей Системы не должен сказываться на общей функциональности остальной части Системы.

4.6.2. В рамках разработки или модернизации Системы должны быть выстроены процессы резервного копирования и восстановления данных, обрабатываемых в Системе.

4.6.3. Процесс резервного копирования не должен работать с резервируемыми данными в монопольном режиме.

4.6.4. В случае резервирования критичных данных резервная копия должна шифроваться.

4.7. Требования к эксплуатации

4.7.1. Перевод Системы в промышленную эксплуатацию или доступ из сети Интернет возможен только после проведения ДИБ аудита ИБ и получения положительного заключения по результатам такого аудита.

Шаблон заявки на проведение аудита размещен на корпоративном портале.

4.7.2. Проектирование ИС должно производиться на последних мажорных версиях программного обеспечения, кроме случаев необходимости

использования сертифицированных версий или конфликта версий между разными компонентами ИС или с другими ИС.

При вводе в эксплуатацию ИС ОС серверов и компоненты ИС должны обновляться согласно Регламенту установки обновлений ОС Windows и прикладного программного обеспечения.

4.7.3. Обновления Системы должны проходить тестирование перед установкой в продуктивной среде.

4.7.4. В случае возникновения нестабильной работы Системы в результате установки обновлений безопасности организация, осуществляющая поддержку Системы, должна предложить и внедрить альтернативное решение возникшей проблемы в соответствии с действующим соглашением об уровне предоставления услуги (SLA).

4.7.5. Разработка и тестирование изменений Системы не должны выполняться на продуктивных экземплярах Системы. Установка средств разработки (компиляторы, отладчики, шестнадцатеричные редакторы и т.п.) и тестирования на продуктивных экземплярах Системы запрещена.

4.7.6. Компоненты Системы должны обеспечиваться действующей технической поддержкой на ОС, СУБД, приложения и оборудование.

4.7.7. Все компоненты Системы должны быть зарегистрированы в корпоративных системах мониторинга и управления конфигурациями.

4.7.8. В Системе, находящейся в промышленной эксплуатации, должен быть отключен детальный вывод отладочной информации об ошибках в Системе и ее компонентах, используемой в процессе разработки Системы.

4.7.9. Удаленный административный доступ к Системе и ее компонентам допускается в случае производственной необходимости только из корпоративной сети по защищенным протоколам (SSH-2, SFTP, FTPS, SCP, RDP не ниже версии 6.0 и т.п.).

4.7.10. Пароли от предустановленных учетных записей в продуктивной Системе и ее компонентах должны быть изменены сразу после их установки.

4.7.11. Доступ пользователей к Системе должен регламентироваться соответствующими локальными нормативными актами и предоставляться на основе заявок.

4.7.12. Административный доступ должен предоставляться только администраторам Системы на основании их должностных обязанностей и заявок на предоставление доступа.

4.7.13. На продуктивной Системе учетные записи разработчиков и / или производителей должны быть удалены или заблокированы администраторами Системы.

4.8. Требования к web-приложениям

4.8.1. При разработке или модернизации Системы, содержащей web-интерфейсы или приложения, предъявляются дополнительные требования (**Ошибка! Источник ссылки не найден.** к Стандарту).

4.9. Требования к мобильным приложениям

4.9.1. К разработке или модернизации мобильных приложений предъявляются дополнительные требования (Приложение № 3 к Стандарту).

4.10. Требования к документации

В рамках работ по разработке или модернизации Системы должны быть разработаны или скорректированы документы, содержащие следующую информацию:

4.10.1. Описание Системы:

4.10.1.1. Общие сведения о Системе:

– краткое описание и назначение Системы;

– перечень категорий сведений, обрабатываемых Системой, с указанием степени их конфиденциальности и принадлежности к ПДн, и места хранения (перечень файлов, таблиц / схем СУБД и т.п.).

4.10.1.2. Описание архитектуры Системы:

– сведения о логической структуре и о составе Системы (модули, компоненты);

– описание технологического процесса обработки данных;

– описание структуры программного обеспечения, комплектности и выполняемых функций, включая внешнюю спецификацию каждого включенного в нее модуля;

– описание протоколов обмена, схемы интеграций;

– описание механизма интеграции с другими Системами;

– перечень интерфейсов и перечень команд для каждого интерфейса[1].

4.10.1.3. Инвентаризационные сведения о Системе:

– схема сетевой архитектуры Системы (**Ошибка! Источник ссылки не найден.** к Стандарту);

– таблица IP адресов компонентов Системы (Приложение № 3 к Стандарту);

таблица информационных потоков / доступов Системы (

[1] Указанные сведения могут не включаться в описание для используемых в составе Систем готовых программных и аппаратных продуктов (свободно распространяемых и проприетарных).

– Приложение № 4 к Стандарту);

– перечень используемых типов и версий ОС;

– описание базы данных (логическая структуры)[1];

– описание типов и версий компонентов Системы;

– список компонентов и сервисов ОС, необходимых для работы Системы;

– параметры настроек программного и аппаратного обеспечения, входящих в состав Системы или используемых Системой в качестве поставщика сервиса и необходимых для корректного функционирования Системы;

– перечень папок и файлов, относящихся к приложению, с контрольными суммами для статических файлов;

– перечень ключей и основных параметров реестра, относящихся к приложению[1];

– перечень запускаемых после перезагрузки ОС процессов и сервисов приложения;

– реестр ролей и полномочий Системы (описание групп и ролей пользователей с принадлежностью к подразделениям Общества).

4.10.1.4. Сведения об обеспечении ИБ:

– описание реализации выполнения требований настоящего Стандарта (**Ошибка! Источник ссылки не найден.** к Стандарту) с приложением согласования неприменимости или неисполнения (если требования пункта не учтены) требований с ДИБ;

– перечень и краткое описание используемых средств защиты информации;

– описание исполнения требований эксплуатационной документации на средства защиты информации;

– сведения о протоколируемых событиях ИБ.

4.10.2. Руководство пользователя Системы (для внутренних пользователей).

4.10.3. Руководство администратора Системы.

4.10.4. Матрица доступа Системы.

Матрица доступа представляет собой перечень ролей с указанием лиц / должностей / структурных единиц / структурных подразделений, которым роли могут быть присвоены.

4.10.5. Регламент технического обслуживания.

4.10.6. Схема резервного копирования данных.

4.10.7. Регламент восстановления Системы при сбоях.

4.10.8. Документация, указанная в данном разделе, должна быть доступна только авторизованным пользователям в рамках служебной необходимости. В документации должна отсутствовать аутентификационная информация (пароли и т.п.).

4.10.9. Исходные коды Системы не должны находиться в свободном доступе, если это не противоречит лицензии, по которой распространяется Система.

4.11. Требования к ИСПДн

4.11.1. Системы, обрабатывающие ПДн, должны соответствовать требованиям законодательства Российской Федерации.

4.11.2. В целях минимизации затрат на обеспечение соответствия регуляторным требованиям разрабатываемые или модернизируемые Системы должны соответствовать типовой модели угроз ПДн, утвержденной в Обществе.

В случае несоответствия разрабатываемой или модернизируемой Системы типовой модели угроз ПДн рекомендуется применить компенсирующие меры, например, изменить объем обрабатываемых ПДн, их категорию, применить обезличивание (как обратимое, так и необратимое), с целью приведения в соответствие архитектурных решений Системы типовой модели угроз.

При соответствии разрабатываемой или модернизируемой Системы типовой модели угроз защита ПДн осуществляется развернутой в Обществе системой защиты ПДн, обеспечивающей для серверных компонент 3 уровень защищенности, а для пользовательских компонент – 4 уровень защищенности.

В случае неприменимости типовой модели угроз ПДн к разрабатываемой и модернизируемой Системе даже с учетом корректировки ее архитектурных решений в рамках работ по разработке или модернизации Системы необходимо:

- разработать частную модель угроз ПДн на основе типовой модели;
- разработать проект защиты ПДн, обрабатываемых в Системе, соответствующий частной модели угроз, с учетом использования решений развернутой в Обществе системы защиты ПДн;
- внедрить проект защиты ПДн разрабатываемой или модернизируемой Системы.

4.11.3. Обезличивание информации может осуществляться в соответствии с приказом Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и Методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденных руководителем Роскомнадзора 13.12.2013.

5. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ РАБОТ

5.1. В случае разработки или модернизации Системы, использующей средства криптографической защиты информации (СКЗИ), исполнитель должен обладать лицензией на выполнение работ, связанных с СКЗИ, и разработать предложения по выполнению требований приказа ФАПСИ от 13.06.2001 № 152.

5.2. В случае разработки или модернизации Системы, использующей сертифицированные средства защиты информации, исполнитель должен обладать лицензией ФСТЭК России на выполнение соответствующих работ.

5.3. В случае интеграции Системы с другими информационными системами или использования любого состава и комбинаций технических и / или программных средств, обслуживаемых и / или закупаемых Обществом для обеспечения функционирования разрабатываемой Системы и не входящих в ее состав, Исполнитель должен предоставить комплексное решение по обеспечению ИБ, включая предложения по настройке, размещению и эксплуатации указанных выше средств начиная от каналообразующего оборудования и заканчивая прикладным программным обеспечением.

Приложение № 1
к Стандарту

Список рекомендуемых криптографических алгоритмов

1. Симметричные алгоритмы шифрования:
   - AES (согласно FIPS 197).
   - ГОСТ Р 34.12-2015.

2. Асимметричные алгоритмы шифрования и ЭП:
   - Согласно ГОСТ Р 34.10-2012.
   - RSA (реализация согласно ISO/IEC 14888-2:2008, FIPS 186-4 и IEEE P1363).
   - ECDSA (реализация согласно ISO/IEC 14888-3, IEEE P1363, FIPS 186-4 и ANSI X9.62-2005).
   - DSA (согласно FIPS 186-4).
   - ElGamal.

3. Алгоритмы обмена ключевым материалом:
   - Diffie-Hellman.
   - Реализация согласно Рекомендациям по стандартизации ТК-026.

4. Алгоритмы хеширования (требуется использовать соль – модификатор входных данных хеш-функции):
   - Согласно ГОСТ Р 34.11-2012;
   - SHA-2 (SHA-224, SHA-256, SHA-384 и SHA-512);
   - SHA-3 (согласно FIPS 202).
   - Стрибог (реализация согласно ГОСТ Р 34.11-2012).

Приложение № 2
к Стандарту

Требования к WEB-приложениям

1. Требования к HTTP-заголовкам

Ниже приведен перечень HTTP-заголовков, применение которых обязательно для всех разрабатываемых или модернизируемых web-приложений.

1.1. «Strict-Transport-Security»

Устанавливает срок, в течение которого при переходе на сайт браузер должен использовать только протокол HTTPS. Защищает от downgrade-атак и атак «MiTM».

Заголовок необходимо использовать только для сайтов, обменивающихся данными по протоколу HTTPS. Срок использования HTTPS должен быть не менее 1 года: «**max-age: 31536000**».

1.2. «X-Frame-Options»

Задает параметры использования контента web-приложения в iframe, предотвращая Clickjacking атаки.

В случае, если контент не передается, необходимо использовать параметр «**X-Frame-Options: deny**». В случае передачи контента в Iframe необходимо использовать параметр «**X-Frame-Options: sameorigin**».

1.3. «X-XSS-Protection»

Активирует встроенную защиту браузера от XSS-атак.

Для активации защиты используются следующие параметры: «**X-XSS-Protection: 1; mode=block**».

1.4. «X-Content-Type-Options»

Предотвращает выполнение в браузере активного содержимого, для которого не задан или неверно задан тип контента.

Для активации защиты используется параметр «**X-Content-Type-Options: nosniff**».

1.5. «Referrer-Policy»

Определяет, какая информация передается в заголовке «Referer» при переходе на другую страницу. Предотвращает передачу информации при переходе на другие сайты.

Если информация не должна передаваться, задается значение «**Referrer-Policy: no-referrer**». Если информация передается в пределах одного сайта – «**Referrer-Policy: same-origin**».

1.6. «Feature-Policy»

Определяет, какие функции и API браузера могут использоваться на сайте (камера, геолокация, микрофон и др.). Обеспечивает защиту от сбора данных о пользователях.

Если функции «**camera**», «**geolocation**», «**microphone**», «**payment**», «**speaker**», «**vibrate**» и «**usb**» не используются, для них должно быть задано значение «**none**».

1.7. «Content-Security-Policy»

Задает политику безопасности контента. Перед применением заголовка «Content-Security-Policy:» в продуктивной среде рекомендуется:

– Применение заголовка «Content-Security-Policy:» в тестовой среде или в среде разработки.

– Применение заголовка «Content-Security-Policy-Report-Only:» в продуктивной среде. Данный заголовок производит запись работы директив вместо их применения, что позволяет проверить их работу.

1.7.1. Директива «default-src» – разрешенные источники по умолчанию для остальных директив.

Использование «default-src *» запрещено.

1.7.2. Директива «script-src» – источники, с которых допускается исполнение скриптов.

Использование «script-src *» запрещено.

1.7.3. Директива «style-src» – источники, с которых допускается загрузка таблиц стилей.

Использование «style-src *» запрещено.

1.7.4. Другие директивы

В случае, если перечень возможных источников других объектов (изображения, аудио, видео, шрифты и др.) полностью не совпадает с перечнем директивы «default-src», необходимо использовать соответствующую объекту директиву.

1.7.5. Параметр «report-uri»

Данный параметр задает адрес, на который браузер направляет отчет в случае нарушения политики.

В целях ускорения решения проблем рекомендуется включение данной директивы в политику.

1.7.6. Использование параметра «nonce»

Данный параметр используется в случаях, когда невозможно указать конкретный URL **внутреннего или внешнего** источника (для скрипта или стиля).

Требования к значениям «nonce»:

– Сервер создает новое уникальное значение каждый раз при передаче политики.

– Значение должно быть длиной более 128 бит (до кодирования).

– Для создания значения должен использоваться криптографически безопасный генератор случайных чисел.

– Значение не должно являться хэшем или цифровой подписью скрипта (так как они не являются случайными).

1.7.7. Использование параметра «hash»

Данный параметр используется в случаях, когда невозможно указать конкретный URL **внутреннего** источника (для скрипта или стиля) или использовать параметр «nonce».

Для вычисления значения хэша рекомендуется использовать алгоритм SHA512.

1.7.8. Использование параметра «'unsafe-inline'»

Данный параметр используется только в случаях, когда невозможно избежать использования встроенных скриптов.

1.7.9. Использование параметра «'unsafe-eval'»

Данный параметр используется только в случаях, когда невозможно избежать использования функции «eval()» в коде скрипта.

2. Требования к активному содержимому и скриптам

2.1. Общие требования

Исходный код скриптов и активных компонент, исполняемых на клиентской стороне (сценарии JavaScript, AJAX, ActiveX, Java-апплеты и т.д.), не должен содержать сведений конфиденциального характера (специфических алгоритмов, паролей, критичных переменных и т.д.).

2.2. Требования к сценариям AJAX (Asynchronous JavaScript and XML)

2.2.1. Использование технологии AJAX для обработки платежной информации запрещено.

2.3. Требования к сценариям JavaScript

2.3.1. Структуры и данные, обеспечивающие безопасность web-приложения (токены аутентификации, сессионные cookie и т.д.) не должны обрабатываться сценариями JavaScript.

2.3.2. Рекомендуется использовать JavaScript-сценарии из системы хранения исходного кода Общества или создавать собственные сценарии на основе таких. Использование собственных сценариев JavaScript по возможности должно быть сведено к минимуму.

2.4. Требования к ActiveX и сценариям Visual Basic

2.4.1. Использование скриптов, написанных на Visual Basic, запрещено.

2.4.2. Использовать компоненты ActiveX не рекомендуется.

2.5. Требования к Java-апплетам

2.5.1. Все используемые Java-апплеты должны иметь цифровую подпись доверенного удостоверяющего центра.

2.5.2. Java-апплет не является доверенным компонентом. В связи с этим в коде апплета не должны быть реализованы механизмы принятия критичных решений (например, относящимся к механизмам безопасности или бизнес процессам).

2.5.3. Рекомендуется использовать обфускацию байт-кода Java-апплетов.

3. Требования к проверке входных и выходных параметров

3.1. Все входные параметры должны проверяться на серверной стороне с целью выявления распространенных сценариев атак на web-приложения (XSS, SQL-инъекции, CSRF и т.д.). Например, поле с ФИО не должно принимать в обработку данные, содержащие цифры или знаки препинания.

3.2. Проверка входных параметров должна осуществляться до их использования компонентами web-приложения (базы данных, скрипты и т.д.).

3.3. Web-приложение должно проверять полноту полученных от пользователя параметров (например, наличие всех параметров в форме ввода).

3.4. HTTP-заголовки и скрытые HTML-поля (<input type=hidden>), если они используются в web-приложении, должны проходить проверку, как и обычные HTTP-параметры.

3.5. Сообщения об ошибках не должны содержать сведений, по которым возможно восстановить метод проверки параметров.

3.6. Рекомендуется дополнительно осуществлять проверку входных параметров от пользователя в клиентской части web-приложения.

3.7. Очистка возвращаемых данных

3.7.1. Проверка возвращаемых пользователю данных должна осуществляться до момента отправки web-страницы от сервера браузеру.

3.7.2. Форматирование выводимой пользователю HTML-разметки должно осуществляться средствами CMS или доверенных библиотек (например, функция «htmlspecialchars» в PHP). Запрещается использовать HTML-теги из входных данных пользователя для формирования web-страниц (сообщения на форумах, гостевых книгах и т.д.).

3.7.3. В случае необходимости визуализировать управляющие символы, используемые в HTML, JavaScript, Flash и других компонентах, серверная часть web-приложения должна осуществлять замену всех управляющих символов на их «видимые» аналоги (<script> на <script> и т.д.).

4. Предотвращение раскрытия информации

4.1. Передача учетных данных

4.1.1. Передача учетных данных пользователя и другой аутентификационной информации должна осуществляться по защищенному протоколу TLS.

4.2. Минимизация вывода информации

4.2.1. Исходный код web-страниц не должен содержать служебную информацию. Например, комментарии, мета-теги, скрытые поля, cookies не должны содержать сведения, которые могут быть использованы для подготовки атак (внутренние IP-адреса, телефоны, адреса электронной почты, описания работы алгоритмов и т.д.).

4.2.2. Сообщения об ошибках не должны содержать информации о версии программного обеспечения, используемого Системой, внутренних путей, а также ранее введенных пользователем данных.

4.2.3. Web-серверы, СУБД и используемые приложения должны быть сконфигурированы таким образом, чтобы затруднить атакующему определение реальных версий компонентов.

4.3. Требования к формированию URL

4.3.1. URL не должны содержать сведений конфиденциального характера (IP-адреса, пароли, номера кредитных карт, ФИО и т.д.).

4.3.2. Передача конфиденциальных данных должна осуществляться с помощью метода «POST». Запрещается использование метода «GET» для передачи сведений конфиденциального характера. Возможность использования «GET» API-интерфейсами, передающими конфиденциальные данные, необходимо определять в соответствии с архитектурой Системы, критичностью передаваемых данных, количеством пользователей и др. параметрами, характерными для конкретного случая.

4.3.3. Запрещается использование «секретных» HTTP-параметров (debug=true, admin=1 и т.д.) для перевода web-приложения в режим отладки, администрирования или получения доступа к неподдерживаемому в обычном режиме функционалу.

4.3.4. Запрещается передавать конфиденциальные данные в рамках перенаправления (редиректа) на другие web-ресурсы.

5. Требования к сессиям

5.1. Требования к идентификаторам сессий (Session ID)

5.1.1. Идентификатор сессии должен быть уникальным и не предугадываемым. Запрещается использование идентификаторов сессий, сформированных с помощью простого или известного алгоритма (инкрементирование, системное время и т.д.).

5.1.2. Идентификатор сессии должен быть устойчив к подбору. Длина идентификатора сессии должна быть не менее 128 бит.

5.1.3. Идентификатор сессии не должен зависеть от других идентификаторов (сформированных ранее), имени пользователя, пароля, состояния приложения.

5.1.4. Клиентская часть web-приложения не должна иметь возможность изменять идентификатор сессии.

5.1.5. В случае, когда web-приложение использует TLS для передачи данных, идентификатор сессии всегда должен передаваться внутри защищенного соединения.

5.1.6. Новый идентификатор сессии должен формироваться приложением каждый раз после прохождения успешной аутентификации пользователя. В случае, если пользователь в процессе аутентификации передает заранее сформированный идентификатор сессии, он должен быть проигнорирован. Данное требование существует в целях исключения влияния пользователя на процесс генерации идентификатора сессии.

5.2. Управление сессиями

5.2.1. Время жизни сессий должно быть ограничено. По истечении данного времени, сессия должна быть удалена или должен быть сгенерирован новый запрос на обновление аутентификации. Значение необходимо определять в соответствии с критичностью передаваемых данных, количества пользователей и других параметров, характерных для конкретного случая.

5.2.2. Неактивные сессии должны завершаться автоматически. Время завершения сессии настраивается в зависимости от функционала web-приложения, количества пользователей, критичности обрабатываемых ресурсов. Рекомендуемое значение для административных консолей – 5 мин, для пользовательского web-интерфейса 30 мин.

5.2.3. Web-приложение на клиентской стороне не должно искусственно поддерживать сессию в активном состоянии, предотвращая ее автоматическое завершение по таймауту неактивности.

5.2.4. Необходимо использовать встроенные в стандартные библиотеки и механизмы управления сессиями в случае наличия таковых. Реализация собственных механизмов управления сессиями не рекомендуется.

5.2.5. Для предотвращения кражи или модификации данных о сессиях пользователей web-приложения, эти данные должны храниться в месте не доступном для других приложений и систем (в том случае, если они не защищены другим способом, например, путем шифрования). К недопустимым местам хранения, в частности, относятся общие папки с временными файлами на web-сервере.

5.2.6. Разрешается использование 2-х ступенчатых механизмов, когда web-приложение с помощью постоянных cookies помнит некоторые настройки пользователя и применяет их при следующем посещении. Однако для доступа к ПДн или совершения транзакций по-прежнему требуется прохождение стандартной процедуры аутентификации и проверки прав.

5.2.7. Возможность использования механизмов «запомнить меня» для включения механизма автоматической аутентификации необходимо определять в соответствие с критичностью передаваемых данных, количества пользователей и других параметров, характерных для конкретного случая.

5.2.8. В случае, если web-приложение использует клиентские сертификаты для аутентификации пользователей (или другие механизмы, при которых кража идентификатора сессии не ведет к получению доступа в контексте пользователя приложения), могут быть установлены специальные требования к механизму управления сессиями.

5.3. Завершение сессий

5.3.1. Web-приложение должно содержать механизм завершения сессии (кнопка «выход»), доступный пользователю из любой страницы приложения.

5.3.2. По завершении сессии относящиеся к ней конфиденциальные данные должны быть полностью удалены на серверной стороне.

5.3.3. Сессия, содержащая конфиденциальные данные, должна автоматически завершаться при закрытии браузера.

5.3.4. Рекомендуется удалять сессионные данные на ПК клиента.

6. Требования к использованию протокола HTTP

6.1. Требуется использовать протокол HTTPS. Использование протокола HTTP допускается в следующих случаях:

– при передаче информации в пределах одного сегмента сети;

– при передаче информации, не содержащей сведений, составляющих коммерческую тайну и иную конфиденциальную информацию.

6.2. Web-приложение должно поддерживать минимально необходимый набор HTTP-методов. Неиспользуемые HTTP-методы должны быть отключены на web-сервере, а попытки их использования должны игнорироваться.

6.3. Требования к использованию cookies

6.3.1. Атрибут «HTTPOnly» должен быть установлен значением «true».

6.3.2. В случае использования протокола HTTPS должен быть установлен флаг «secure».

6.3.3. Атрибут «domain» должен быть установлен значением только того ресурса, для которого требуется поддержка данного cookie. Например, если приложение располагается на домене «info.pochta.ru», то связанный с ним cookie должен иметь значение параметра «domain=info.pochta.ru», а не «domain=.pochta.ru».

6.3.4. Атрибут «path» должен быть настроен таким образом, чтобы браузер пользователя отправлял cookies только тому web-приложению, которому они предназначаются.

7. Требования к HTML

7.1. Требования к комментариям и скрытым полям HTML

7.1.1. HTML-комментарии не должны содержать внутреннюю информацию web-приложения (IP-адреса, логины, пароли, адреса электронной почты, телефоны) а также раскрывать особенности реализации Системы.

7.1.2. В скрытых полях HTML-страниц в незашифрованном виде запрещается передавать конфиденциальные сведения (номера кредитных карт, номера телефонов и т.д.), аутентификационную информацию (имя пользователя, пароль, токен аутентификации), а также управляющие команды, которые могут нарушить работу web-приложения (теги, SQL-операторы, shell-команды).

7.2. Требования к всплывающим окнам (pop-up)

7.2.1. Использование всплывающих окон (pop-up) для реализации логики web-приложений должно быть ограничено. В случае крайней

необходимости всплывающие окна должны использоваться только для отображения информационных сообщений.

7.2.2. Запрещается использование всплывающих окон для получения данных от пользователя.

8. Криптография

8.1. В случае, если web-приложение использует HTTPS для защиты взаимодействия с клиентом, доступ к ресурсам по HTTP должен быть запрещен. В качестве криптографического протокола необходимо использовать TLS не ниже v.1.2.

8.2. В случае перенаправления пользователя с защищенных ресурсов web-приложения (доступных только по HTTPS) на незащищенные (доступные по HTTP) сессия клиента должна быть либо завершена, либо должны быть удалены конфиденциальные данные, используемые в рамках сессии. Подобные обстоятельства возникают в случае если часть ресурсов web-приложения доступна по HTTP, а часть защищена HTTPS, чего в обычной практике лучше избегать. Рекомендуемая мера не позволяет атакующему получить доступ по HTTP к web-страницам, защищенным HTTPS.

8.3. Конфиденциальная информация (например, пароли, детализации разговоров, финансовые отчеты, ПДн и др.) должна передаваться только по защищенному протоколу HTTPS.

8.4. Использование гиперссылок, перенаправляющих с защищенных web-страниц приложения (доступных только по HTTPS) на незащищенные, не должно приводить к появлению конфиденциальных сведений в поле «HTTP-referer».

9. Требования к архитектуре

9.1. Требования к регистрации пользователей

9.1.1. Форма регистрации клиентов в web-приложении должна быть защищена от автоматических средств регистрации (CAPTCHA или альтернативные решения для защиты).

9.2. Требования к контролю состояний процессов

9.2.1. Web-приложение должно контролировать состояние, на котором находится клиент. Нелегитимные переходы между состояниями процессов должны быть заблокированы (переход к оплате без выбора товара или заполнения данных о клиенте и т.д.).

9.2.2. Рекомендуется реализовывать механизм контроля состояний процессов на серверной стороне web-приложения.

9.2.3. Индикатор состояния должен быть уникальным и не являться предугадываемым.

9.2.4. Запрещается использовать содержимое HTTP-referer для контроля состояния процессов.

9.3. Скрытые и замаскированные ресурсы

9.3.1. Все страницы и активные скрипты web-сервера, к которым пользователь может получить доступ, должны быть частью web-приложения.

Пользователю не должны быть доступны web-страницы, директории, файлы, непосредственно не принадлежащие приложению, а также:

- файлы резервных копий (например, *.old, *.bak);
- файлы баз-данных (например, *.db, *.sqlite, *.accdb);
- лог-файлы;
- временные директории;
- исходные коды и директории SVN;
- используемые библиотеки.

9.3.2. Запрещается ограничивать доступ к файлам путем переименования файлов или путем не указания гиперссылок на них.

9.3.3. Запрещается оставлять неиспользуемые директории и файлы на продуктивном сервере (например, файл login.php.old или директория jsp.old).

9.4. Требования к аутентификации

9.4.1. Учетные данные не должны храниться в местах, доступных для клиента (cookies, URL, исходный код и т.д.).

9.4.2. Процесс аутентификации не должен основываться на данных и переменных, которые можно легко модифицировать (HTTP заголовки, user-agent, HTTP-referer и т.д.).

9.4.3. При начальной регистрации пользователя или восстановлении утерянного пароля необходимо предусмотреть возможность проверки его сложности.

9.4.4. Для доступа к разделам, связанным с пользовательской информацией и выполнением действий от лица пользователя, необходима обязательная аутентификация.

9.4.5. Процедура аутентификации должна иметь защиту от подбора паролей (CAPTCHA, задержка на повторный ввод или временный запрет на доступ). Количество неудачных попыток ввода пароля и время блокировки повторного ввода пароля должны быть настраиваемыми параметрами с стороны администратора Системы.

9.5. Требования к авторизации

9.5.1. Web-сервер, на котором работают web-приложения и сервер СУБД (по возможности), должен быть запущен под специально созданной технологической учетной записью ОС с минимально необходимым набором привилегий. Запуск web-сервера под системными учетными записями (например, root или LOCALSYSTEM) может вести к серьезным уязвимостям.

9.5.2. Для предотвращения полной компрометации сервера в случае взлома web-приложения учетной записи СУБД, под которой работает web-приложение, необходимо предоставлять ограниченные права на работу с файловой системой сервера (на функции создания, чтения, удаления, изменения файлов), а также на исполнение команд ОС с помощью вызова хранимых процедур или путем использования библиотек.

9.6. Взаимодействие между компонентами

9.6.1. При обращении к базам данных web-приложения должны использовать хранимые процедуры вместо SQL-запросов, содержащих параметры.

9.6.2. Хранение паролей в БД web-приложения должно осуществляться с использованием криптографических алгоритмов, определяемых в соответствии с пунктом 4.1.1 Стандарта.

9.6.3. Доступ к web-интерфейсам администрирования web-приложений из сети Интернет должен быть запрещен.

9.6.4. Административные и пользовательские интерфейсы должны быть разделены. Пользовательский интерфейс не должен предоставлять возможностей администрирования Системы.

9.6.5. Web-интерфейсы систем мониторинга (например, Nagios, Zabbix, Cacti, Munin и др.) не должны быть доступны из сети Интернет.

9.7. Контроль состояния клиента

9.7.1. Должен использоваться механизм контроля состояния клиента, путем присвоения клиенту начального идентификатора состояния (при начале работы с приложением) и его последовательного изменения в процессе работы. При этом клиенту передается зашифрованный параметр (токен), содержащий сведения о текущем состоянии клиента, который в свою очередь передается серверу при каждом обращении.

9.7.2. Если механизм управления состоянием используется на стороне клиента, параметр контроля состояния клиента (идентификатор состояния или токен) должен быть зашифрован.

9.8. Сокрытие внутренней структуры

9.8.1. В целях сокрытия внутренней информации web-приложения от злоумышленников (структуры приложения, правил именования файлов) запрещается использовать прямое, легко угадываемое именование содержимого (например, Report-2013.xls, Report-2014.xls и т.д.).

9.8.2. Необходимо контролировать отсутствие информации о внутренней структуре Системы или сети Общества в ответах и страницах web-приложений Системы.

10. Требования к API

10.1. Структура запросов к API должна быть задокументирована, включая все возможные значения принимаемых параметров.

10.2. Для каждой функции должна быть реализована авторизация.

10.3. Количество субъектов, данные по которым могут отдаваться в одном ответе, рекомендуется ограничить.

Количество субъектов определяется на этапе тестирования исходя из планируемых мощностей и нагрузки.

10.4. Система должна отдавать по API только те данные, которые были запрошены.

10.5. Требования к «секрету»

10.5.1. Для аутентификации подключаемых систем должен использоваться «секрет»: токен или ключ доступа.

10.5.2. «Секрет» не должен быть внедрен в код системы.

10.5.3. «Секрет» должен быть доступен только для использования конкретной системой-клиентом (привязка по IP).

10.5.4. Срок действия «секрета» не должен превышать 1 года.

Приложение № 3
к Стандарту

Требования к мобильным приложениям

1. Термины и определения

В настоящем приложении к Стандарту используются следующие термины и определения.

№	Наименование термина	Перевод	Определение термина (расшифровка сокращения)
1	**Activity**	Активность	Компонент приложения с отдельным экраном.
2	**Application component**	Компонент приложения	Компоненты, из которых состоит приложение: Activity, Intent.
2.1	Private component	Внутренний компонент	Компонент, доступный для вызова только самим приложением.
2.2	In-house component	Доверенный компонент	Компонент, доступный для вызова только приложениями того же разработчика.
2.3	Partner component	Партнерский компонент	Компонент, доступный для вызова только приложениями-партнерами.
2.4	Third party component	Сторонний компонент	Компонент, принадлежащий операционной системе или другому приложению.
3	**Automatic reference counting (ARC)**		Функция управления памятью компилятора Clang, обеспечивающая автоматический подсчет ссылок для языков программирования Objective-C и Swift.
4	**Backup**	Резервная копия	
4.1	Application Backup	Резервная копия приложения	Резервная копия, включающая все данные приложения.
5	**Binding**	Привязка	Привязка приложения к какому-либо параметру устройства.
6	**Clipboard**	Буфер обмена	Область памяти, предназначенная для переноса информации между приложениями или частями одного приложения с использованием функций "Копировать", "Вырезать" и "Вставить".
7	**Intent**		Механизм взаимодействия приложений.
7.1	Явный Intent		Intent, в котором указано конкретное приложение для запуска.
8	**Inter-process communication (IPC)**	Межпроцессное взаимодействие	Механизм операционной системы, позволяющий потокам одного или разных процессов обмениваться данными.

№	Наименование термина	Перевод	Определение термина (расшифровка сокращения)
9	**Keyboard cache**	Кэш клавиатуры	Данные, введенные пользователем с помощью приложения «клавиатура», сохраненные для улучшения работы приложения (обучение автозаполнения, словарь и т.п.).
10	**Keystore**	Хранилище ключей	Контейнер для хранения криптографических ключей, затрудняющий несанкционированный доступ к ним.
11	**Notification**	Уведомление	Короткое сообщение в строке состояния устройства.
11.1	Public notification	Небезопасное уведомление	Версия (вариант) уведомления, которое будет отображаться в небезопасном окружении (к примеру, на заблокированном экране).
12	**Protocol**	Протокол	Правила, позволяющие двум и более системам обмениваться информацией.
12.1	«File» protocol	Протокол «file»	Протокол для взаимодействия с файлами.
12.2	«Tel» protocol	Протокол «tel»	Протокол для осуществления звонков.
12.3	«App-id» protocol	Протокол «app-id»	Протокол для вызова других приложений.
13	**Pseudorandom number generator (PRNG)**	Генератор случайных чисел (ГСЧ)	Алгоритм, генерирующий последовательность чисел, которые почти независимы друг от друга и подчиняются заданному математическому распределению (обычно равномерному).
13.1	Cryptographically secure PRNG	Криптографически стойкий ГСЧ	Генератор псевдослучайных чисел, обладающий свойствами, позволяющими использовать его в криптографии.
14	**Release версия**	Продуктивная версия	Версия приложения, предназначенная для пользователей системы.
15	**Root**	Права администратора	
15.1	Наличие root на устройстве		Наличие прав администратора у учетной записи, с помощью которой работает пользователь.
16	**Same Origin Policy (SOP)**		Механизм безопасности, который ограничивает взаимодействие документа или сценария, загруженного из одного источника, с ресурсом из другого источника.
17	**SSL pinning**		Внедрение в код мобильного приложения SSL сертификата, который используется на сервере, для последующей проверки сертификата при соединении с сервером.
18	**Stack protection**	Защита стека	Механизм защиты приложения от атаки «stack smashing».

№	Наименование термина	Перевод	Определение термина (расшифровка сокращения)
19	**WebView**		Компонент операционной системы, используемый приложениями для отображения веб-контента (HTML, JS, CSS) в нем самом вместо отображения веб-контента в браузере.
20	**Валидация данных**		Проверка данных на соответствие формату (email, тел. номер, ФИО и др.).
21	**Десериализация данных**		Преобразование входящих данных из битовой последовательности в исходный формат (для использования конкретным компонентом).
22	**Инвалидация сессии**		Отзыв доступов, связанных с пользовательской сессией.
23	**Минификация кода**		Удаление из исходного кода приложения всех символов, не являющихся необходимыми для функционирования приложения.
24	**Санитизация**		Процедура удаления (или экранирования) неправильных или небезопасных для приложения символов.
25	**Экран быстрого доступа**		Экран переключения между приложениями, отображающий снимки Activity приложений.

2. Хранение данных и конфиденциальность

2.1. Работа с ключами шифрования

2.1.1. Используемые в приложении ключи шифрования должны храниться в системном хранилище ключей (к примеру, Android KeyStore или Apple Security Enclave).

2.1.2. Приложение не должно содержать ключи шифрования в исходном коде (hardcoded keys).

2.1.3. Приложение должно использовать ключи шифрования длины не менее: 256 бит – для симметричных шифров, 3072 бит – для асимметричных.

2.1.4. Приложение не должно использовать один и тот же ключ шифрования для нескольких целей.

2.2. Обработка конфиденциальной информации

2.2.1. КИ должна храниться во внутреннем хранилище приложения либо в защищенном системном хранилище данных (к примеру, Keychain для iOS, Apple Security Enclave).

2.2.2. Продуктивная версия приложения не должна сохранять КИ в журнал сбора событий (как журнал приложения, так и системный).

2.2.3. Приложение не должно хранить КИ в памяти дольше, чем это требуется.

2.2.4. Приложение должно удалять КИ из оперативной памяти сразу после окончания работы с ней.

2.2.5. КИ не должна передаваться через механизмы IPC.

2.2.6. Отображение КИ на экране устройства

2.2.6.1. КИ, такая как пароли или пин-код, не должна отображаться в пользовательском интерфейсе.

Рекомендуется использовать маскирование. Допускается использование функции кратковременного отображения пароля или пин-кода.

2.2.6.2. Приложение не должно содержать КИ на экране быстрого доступа (экране переключения между приложениями).

2.2.6.3. Небезопасные уведомления (уведомления на экране заблокированного устройства) не должны содержать КИ.

2.2.7. Конфиденциальная информация в текстовых полях

2.2.7.1. Кэш клавиатуры должен быть отключен для текстовых полей, которые могут содержать КИ (отключено сохранение данных, введенных с помощью приложения «клавиатура»).

2.2.7.2. Буфер обмена должен быть отключен для текстовых полей, которые могут содержать КИ (отключена возможность взаимодействия поля ввода с буфером обмена (функции «Копировать» и «Вырезать»)).

3. Криптография

3.1. Приложение должно использовать только проверенные реализации криптографических алгоритмов (см. Приложение 3 Стандарта).

3.2. Приложение должно явно определять режим (параметры, технологии) шифрования.

3.3. Если приложение использует случайные числа, они должны генерироваться с использованием встроенных функций операционной системы («/dev/urandom» для Android, «SecRandomCopyBytes» для iOS).

3.4. Ключи шифрования не должны храниться в исходном коде.

3.5. Сетевые соединения

3.5.1. Канал связи должен быть защищен с помощью TLS не ниже v.1.2.

Приложение должно запрещать соединение по протоколам SSLv3 и ниже. Шифрование данных должно использоваться для всех сетевых соединений приложения.

3.5.2. Приложение должно использовать актуальные версии библиотек для организации безопасности и установки соединений.

3.6. Требования к работе с сертификатами

3.6.1. Перед установкой TLS-соединения приложение должно проверять сертификат сервера, с которым устанавливается соединение.

Сертификат должен быть подписан доверенным удостоверяющим центром.

3.6.2. Приложение должно проверять, что срок действия и другие свойства сертификата сервера действительны.

3.6.3. Приложение должно проверять, что имя сервера системы соответствует CN (Common Name) или SAN (альтернативные имена объектов) в поле «Subject» сертификата сервера.

3.6.4. Приложение должно использовать свое собственное хранилище сертификатов или механизм SSL Pinning и не устанавливать соединение с серверами, не прошедшими проверку, даже если их сертификат выдан доверенным центром сертификации.

3.6.5. Используемые приложением сертификаты не должны храниться в общедоступных местах.

4. Аутентификация

4.1. Если в приложении обрабатывается КИ, для входа в приложение должна использоваться аутентификация.

4.2. Если используется аутентификация на основе токена, сервер должен предоставлять токен, подписанный с использованием криптографически стойкого алгоритма шифрования (см. приложение № 3 к Стандарту).

4.3. При аутентификации с помощью биометрической информации событие успешной проверки отпечатка должно использоваться для разблокировки ключа в хранилище ключей (KeyStore для Android, keychain для iOS), а не для входа в систему.

4.4. В приложении должна быть настроена парольная политика, параметры которой устанавливаются на сервере.

4.5. Для критичных операций должно запрашиваться дополнительное подтверждение или повторная аутентификация.

4.6. Приложение должно предоставлять пользователю:

– информацию о нескольких последних входах в систему (дата и время входа, продолжительность сессии);

– список использовавшихся для входа устройств (название, модель, IMEI).

4.7. Рекомендуется реализовать в Приложении возможность применения второго фактора аутентификации.

5. Управление сессиями

5.1. Идентификатор сессии должен генерироваться случайным образом.

5.2. При создании идентификатора сессии должен использоваться генератор случайных чисел (см. п.3.3).

5.3. При выходе пользователя из приложения сессия должна быть закрыта (инвалидироваться).

5.4. По истечении заданного срока неактивности пользователя или срока действия токена сессия должна быть закрыта (инвалидироваться) приложением.

6. Взаимодействие с платформой

6.1. Приложение должно запрашивать минимально необходимый набор разрешений (только те разрешения, которые необходимы для работы приложения).

6.2. Приложение должно обеспечивать применение ограничений для доступа к устройству (к примеру, установка пользователем пароля разблокировки устройства).

6.3. Приложение должно валидировать и санитизировать все входные данные из внешних источников и от пользователя на устройстве.

Сюда входят данные из UI, механизмов IPC, данных из файловой системы и сетевых источников.

6.4. Должна быть отключена возможность создания резервной копии приложения или резервная копия не должна содержать КИ.

6.5. Дополнительные требования к объекту «WebView»

6.5.1. В элементе «WebView» должен быть разрешен только обработчик протокола HTTPS (должны быть отключены обработчики таких небезопасных протоколов как file, tel, app-id).

6.5.2. Приложение не должно игнорировать ошибки SSL в WebView.

6.5.3. Если в WebView разрешается использование собственных функций приложения, то приложение должно загружать JavaScript только из ресурсов приложения (необходимо использовать функцию «WebView.loadDataWithBaseURL», которая включает SOP).

6.5.4. JavaScript должен быть отключен в WebView, если в нем нет необходимости.

7. Качество клиентского кода

7.1. Исходные коды приложений для мобильных устройств должны быть проверены на отсутствие актуальных угроз безопасности мобильным приложениям по версии OWASP Mobile TOP 10 (OWASP Mobile Security Project – Top Ten Mobile Risks) и других критических уязвимостей (международный цифровой стандарт «The Digital Standard»).

7.2. Продуктивная версия должна быть подписана действующим сертификатом.

7.3. Продуктивная версия приложения должна быть скомпилирована в режиме «release». Должны быть установлены параметры для продуктивных приложений (к примеру, включен параметр «non-debugable», отключен параметр «debugable»).

7.4. Отладочная информация должна быть удалена из бинарных файлов приложения.

7.5. Приложение должно перехватывать и обрабатывать возможные исключения.

7.6. Приложение не должно записывать и хранить подробные сведения об ошибке и отладочные сообщения в штатном режиме работы.

7.7. Все используемые компоненты приложения (такие как библиотеки и фреймворки) должны быть проверены на наличие уязвимостей.

7.8. В случае сбоя в работе функции предоставления доступа по умолчанию доступ предоставляться не должен.

7.9. Должны быть активированы все стандартные функции безопасности, предусмотренные инструментами разработчика (такие как минификация байт-кода, защита стека и ARC).

8. Противодействие атакам

Требования данного раздела должны применяться при разработке приложений, обрабатывающих КИ.

8.1. Приложение должно реализовывать привязку к устройству. Для привязки должен формироваться отпечаток, основанный на нескольких свойствах, уникальных для устройства.

8.2. Требования к обнаружению атак

Приложение должно использовать несколько механизмов защиты для реализации каждого из требований данного пункта. Рекомендуется использование 2 и более различных механизмов (отложенный запуск, косвенные ответы и т.п.).

8.2.1. Приложение должно определять наличие root или jailbreak на устройстве и реагировать*.

8.2.2. Приложение должно определять работу под отладчиком и реагировать*.

8.2.3. Приложение должно определять установленные на устройстве приложения для reverse engineering и реагировать*.

8.2.4. Приложение должно определять работу на эмуляторе и реагировать*.

8.2.5. Приложение должно определять изменение исполняемых файлов и критичных данных в своей песочнице (своем окружении) и реагировать*.

8.2.6. Приложение должно определять изменение своего кода или данных в оперативной памяти и реагировать*.

*Реакция приложения на обнаруженную атаку может заключаться в уведомлении пользователя, прекращении работы приложения, или другом способе противодействия.

8.3. Требования к обфускации

8.3.1. В приложении должна использоваться обфускация для усложнения анализа приложения при динамическом анализе. Обфускация должна быть применена в том числе к программным механизмам, обеспечивающим защиту.

8.3.2. Если задачей обфускации является защита вычислений, то должен использоваться механизм, который:

- применим для этой задачи;
- защищает от ручной и автоматической де-обфускации;
- учитывает опубликованные по этой теме исследования.

9. Требования к приложениям для Android

9.1. При запуске Activity в идентификатор (URI), устанавливаемый в методе «Intent#setData()», не должна включаться КИ.

9.2. Компонент приложения, который используется только внутри приложения, должен быть «Private».

9.3. Для запуска компонента приложения Private, Partner или In-house должен использоваться явный Intent.

Приложение № 4
к Стандарту

Требования к схеме сетевой архитектуры Системы

Схема должна содержать следующие элементы:

- Компоненты ИС, предоставляющие сервис или нуждающиеся в доступе (серверы или кластеры серверов Системы, серверы СУБД, серверы внешних Систем, с которыми взаимодействует внедряемое решение, рабочие станции администраторов, рабочие станции пользователей, сетевое оборудование и другие устройства);
- IP адреса, FQDN компонентов ИС;
- Информационные потоки между компонентами ИС;
- Модели оборудования компонентов ИС.

Приложение № 5
к Стандарту

Образец таблицы IP адресов компонентов Системы

Таблица IP адресов компонентов Системы (IP-план Системы) должна включать следующую информацию:

- IP адрес (IP address) и Тип IP («virtual IP» или «real IP»).
- FQDN.
- VLAN.
- Назначение интерфейса / хоста (Комментарий).

Пример:

IP-адрес	FQDN	VLAN	Комментарий
10.20.444.4	server1.inside.russianpost.ru	ServOS	Адрес сетевой карты первого сервера приложений ИС, используемый для организации IPMP
10.20.444.66	--/--	--/--	Адрес демона IPMP ОС Solaris. Не используется для организации сетевого взаимодействия
10.20.444.12	server2.inside.russianpost.ru	ServOS	Адрес сетевой карты второго сервера приложений ИС, используемый для организации IPMP
10.20.444.68	--/--	--/--	См. 10.20.444.66
10.20.444.70	server3.inside.russianpost.ru	ServOS	Сетевой адрес базы данных Oracle, принимающий подключения от серверов приложений
10.20.246.246	web.russianpost.ru	DMZ	Сетевой адрес внешнего сервера ИС, принимающего подключения от внешних пользователей к web-службам

Приложение № 6
к Стандарту

Требования к таблице информационных потоков / доступов Системы

Таблица информационных потоков / доступов Системы должна включать следующую информацию:

- IP адрес (IP address) и Тип IP («virtual IP» или «real IP»).
- FQDN.
- Входящий или исходящий поток.
- Протокол (TCP, UDP, ICMP и т.п.).
- Номер порта.
- Назначение потока (Комментарий).

FQDN источника	IP источника	NATed IP источника	NATed IP назначения	IP назначения	FQDN назначения	Сетевой протокол	Протокол приложения	Порт источника	Порт назначения	Комментарий
srv5.in.russianpost.ru	10.20.445.8			10.242.8.12	sql5.russianpost.ru	TCP	PL/SQL	Any	1443	Передача данных на сервер агрегации данных
web.russianpost.ru	10.20.246.246			10.242.8.12	web4.russianpost.ru	TCP	HTTP	Any	80	Доступ пользователей к личным кабинетам на web-портале
web2.russianpost.ru	10.20.246.247	172.18.11.114 172.18.11.115 172.18.11.116	172.18.8.12	10.242.8.12	webadm.russianpost.ru	TCP	HTTPS	Any	443	Администрирование web-портала

Приложение № 7
к Стандарту

Описание реализации требований Стандарта

Сведения о системе	
ОС	
СУБД	
Дополнительное ПО	
Обрабатываемые данные, относящиеся к коммерческой тайне и иной конфиденциальной информации Общества (см. приложение № 1 к приказу от 11.11.2010 № 464-п «Перечень …»)	

Исполнение требований	
Раздел "Общие требования"	Требования Стандарта
У	
Раздел "Требования к Web-приложениям"	Требования Приложения 2 к Стандарту
У	
Раздел "Требования к мобильным приложениям"	Требования Приложения 3 к Стандарту
У	

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.1	**Общие требования**	**Требования раздела неприменимы**	**0**	
п.4.1.1	КИ защищена с использованием криптографически стойких алгоритмов шифрования.		<- Выберите	**Высокая**
п.4.1.2	Информация, обеспечение которой определяется законодательством РФ, защищается с использованием СКЗИ, имеющих сертификат соответствия ФСБ России.		<- Выберите	**Высокая**
п.4.1.3	На серверах, расположенных в DMZ, не обрабатывается информация конфиденциального характера.		<- Выберите	**Высокая**
п.4.1.4	В тестовой / учебной среде Системы используются сгенерированные случайным образом данные или обезличенные данные из продуктивной среды.		<- Выберите	**Высокая**
п.4.1.5	Внешние и внутренние интерфейсы Системы разделены.		<- Выберите	**Высокая**
п.4.1.6	Возможность управления сервисами безопасности доступна только администратору Системы.		<- Выберите	**Высокая**
п.4.1.7	**Проверка входных данных**	**Требования раздела неприменимы**	**0**	
п.4.1.7.1	Осуществляется проверка любых входных данных на стороне сервера на длину, допустимые символы, кодировку, полноту данных.		<- Выберите	**Высокая**
п.4.1.7.2	Данные корректируются перед передачей на сервер (удаление лишних символов, приведение к единому формату и т.п.).		<- Выберите	Низкая

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.2	**Требования к аутентификации и авторизации**	**Требования раздела неприменимы**	**0**	
п.4.2.1	Доступ к ресурсам Системы предоставляется после успешного прохождения процесса аутентификации и авторизации.		<- Выберите	**Высокая**
п.4.2.2	Доступ к системе подразделяется на пользовательский, административный, технологический.		<- Выберите	Средняя
п.4.2.3	Реализована ролевая модель доступа.		<- Выберите	**Высокая**
п.4.2.4	Внешняя и внутренняя Системы аутентификации разделены.		<- Выберите	**Высокая**
п.4.2.5	Внутренняя система аутентификации Системы интегрирована с AD или IDM.		<- Выберите	Средняя
п.4.2.6	Каждому пользователю присвоены: идентификатор пользователя; аутентификационная информация; права доступа.		<- Выберите	**Высокая**
п.4.2.7	Каждому пользователю присваивается уникальная учетная запись.		<- Выберите	Средняя
п.4.2.8	Групповые учетные записи не используются.		<- Выберите	Средняя
п.4.2.9	В Системе отсутствуют жестко запрограммированные учетные записи.		<- Выберите	**Высокая**
п.4.2.10	Все неиспользуемые учетные записи удалены или заблокированы.		<- Выберите	**Высокая**
п.4.2.11	В качестве механизма аутентификации используется аутентификация на основе паролей, одноразовых паролей, хранилища ключей или биометрии.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.2.12	Для входа в Систему используется второй фактор аутентификации.		<- Выберите	Низкая
п.4.2.13	Для подтверждения критичных действий в Системе используется повторная аутентификация или аутентификация с помощью второго фактора.		<- Выберите	Низкая
п.4.2.14	Проверка учетных данных осуществляется только после полного их ввода.		<- Выберите	**Высокая**
п.4.2.15	В случае обнаружения ошибки при проверке учетных данных Система не сообщает, какие именно данные введены неправильно (логин или пароль).		<- Выберите	**Высокая**
п.4.2.16	Проверка учетных данных пользователя проводится на стороне серверных компонентов Системы.		<- Выберите	**Высокая**
п.4.2.17	Права доступа могут присваиваться как для доступа к группам данных, так и для выполнения действий в Системе.		<- Выберите	Средняя
п.4.2.18	Соблюден принцип минимизации доступа: всем ролям присвоены права только на те действия в Системе, которые необходимы для данной роли.		<- Выберите	**Высокая**
п.4.2.19	Компоненты Системы проходят процедуру взаимной аутентификации.		<- Выберите	Средняя
п.4.2.20	Реализована защита процессов аутентификации и авторизации от сетевых угроз (пассивное и активное прослушивание сети, подбор паролей и т.п.).		<- Выберите	Средняя
п.4.2.21	До авторизации Система предоставляет пользователю минимальные необходимые данные о себе.		<- Выберите	**Высокая**
п.4.2.22	Пароль не отображается при вводе.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.2.23	**Требования парольной политики**	**Требования раздела неприменимы**	**0**	
п.4.2.23.1	Реализована обязательная смена пароля пользователем при первом входе в Систему		<- Выберите	**Высокая**
п.4.2.23.2	Реализована возможность смены пароля пользователем.		<- Выберите	**Высокая**
п.4.2.23.3	Реализована возможность отключения администратором функции смены паролей для отдельных учетных записей.		<- Выберите	Низкая
п.4.2.23.4	Реализована возможность установки отдельной парольной политики для всех пользователей, для группы пользователей или отдельно для каждой учетной записи.		<- Выберите	Низкая
п.4.2.23.5	Восстановление пароля производится только путем его смены.		<- Выберите	**Высокая**
п.4.2.23.6	Настроена принудительная смена пароля пользователем через установленный промежуток времени.		<- Выберите	**Высокая**
п.4.2.23.7	Оповещение о необходимости изменения пароля настроено.		<- Выберите	Средняя
п.4.2.23.8	Учетная запись блокируется на заранее определенный срок после заданного количества неудачных попыток аутентификации.		<- Выберите	**Высокая**
п.4.2.23.9	Установлена длительность простоя пользовательской сессии, после которой сессия принудительно блокируется.		<- Выберите	Средняя
п.4.2.23.10	Одновременный вход в Систему под одной учетной записью с нескольких устройств запрещен.		<- Выберите	Низкая
п.4.2.23.11	Пароли хранятся и передаются только в зашифрованном виде. При хранении и передаче используются стойкие криптографические алгоритмы или алгоритмы хеширования.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.2.23.12	Вход в Систему заблокирован для учетных записей, срок действия пароля которых истек.		<- Выберите	**Высокая**
п.4.2.23.13	Ведется история паролей (более 12 месяцев): для учетной записи запрещена смена пароля на использовавшийся ранее.		<- Выберите	Средняя
п.4.3	**Требования к сетевому взаимодействию**	**Требования раздела неприменимы**	**0**	
п.4.3.1	Сетевой обмен информацией между компонентами Системы, сопрягаемыми Системами и оборудованием пользователей осуществляется с использованием защищенных стандартов и протоколов.		<- Выберите	**Высокая**
п.4.3.2	DNS-имена (FQDN) внешних компонентов Системы зарегистрированы в прямой и обратной зоне внешних служб DNS. DNS-имена (FQDN) внутренних компонентов Системы зарегистрированы в прямой и обратной зоне внутренних служб DNS.		<- Выберите	Средняя
п.4.3.3	Сетевое взаимодействие Системы и ее компонентов производится с использованием FQDN (не IP-адресов).		<- Выберите	Низкая
п.4.3.4	Ни один из серверов Системы не подключен одновременно к сетевым периметрам с различными уровнями безопасности.		<- Выберите	**Высокая**
п.4.3.5	Доступ к компонентам Системы, размещенным в DMZ, осуществляется с использованием минимально необходимого набора сетевых протоколов и FQDN.		<- Выберите	**Высокая**
п.4.3.6	Серверные компоненты Системы размещены в серверных сегментах сети Предприятия.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.3.7	Продуктивная среда Системы разделена со средой разработки, тестовой средой и беспроводным сегментом на физическом / виртуальном и логическом уровне.		<- Выберите	Средняя
п.4.3.8	**Взаимодействие с интернет**	**Требования раздела неприменимы**	**0**	
п.4.3.8.1	Доступ из сети интернет разрешен только к компонентам Системы, относящимся к продуктивной среде и расположенным в DMZ.		<- Выберите	**Высокая**
п.4.3.8.2	Для организации защищенного удаленного доступа к ресурсам Системы используется централизованный VPN-шлюз Предприятия.		<- Выберите	**Высокая**
п.4.3.8.3	Доступ к сервисам Системы, предназначенным для внутреннего использования, из сети интернет закрыт.		<- Выберите	**Высокая**
п.4.3.8.4	Доступ из сети интернет закрыт к сервисам Системы, использующим для взаимодействия с пользователями протоколы: • SMB/SAMBA/CIFS, NFS, NETBIOS; • доступа к СУБД (MYSQL, MSSQL, ORACLE и др.); • удаленного управления (telnet, SSH, RSH, SNMP, RDP и др.).		<- Выберите	**Высокая**
п.4.3.8.5	Внешние (публичные) интерфейсы Системы размещены в DMZ.		<- Выберите	**Высокая**
п.4.3.8.6	Интернет-сервисы облачного хранения данных не используются в работе Системы.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.4	**Требования к окружению**	**Требования раздела неприменимы**	**0**	
п.4.4.1	Система корректно функционирует с используемыми на Предприятии средствами защиты.		<- Выберите	**Высокая**
п.4.4.2	Система корректно функционирует с используемыми на Предприятии ОС, СУБД и прикладными программами.		<- Выберите	**Высокая**
п.4.4.3	Разрабатываемые компоненты Системы не содержат недокументированных возможностей (НДВ).		<- Выберите	**Высокая**
п.4.4.4	На компонентах Системы запущены только те сервисы и приложения, которые необходимы для ее функционирования.		<- Выберите	Средняя
п.4.4.5	Взаимодействие между компонентами Системы, а также взаимодействие с внешними Системами происходит под технологическими учетными записями с минимально необходимыми наборами привилегий.		<- Выберите	**Высокая**
п.4.4.6	Компоненты Системы построены на продуктах и операционных системах, удовлетворяющих всем требованиям стандартов Предприятия по информационной безопасности.		<- Выберите	**Высокая**
п.4.5	**Требования к аудиту**	**Требования раздела неприменимы**	**0**	
п.4.5.1	Для Системы и ее компонент включен механизм протоколирования событий.		<- Выберите	**Высокая**
п.4.5.2	Механизм протоколирования событий предоставляет возможность сопоставить каждое подлежащее аудиту событие с источником события.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.5.3	Время, указываемое в журналах аудита, синхронизировано с временем NTP-сервера Предприятия.		<- Выберите	Средняя
п.4.5.4	Система имеет возможность фильтрации событий журнала аудита по протоколируемым параметрам.		<- Выберите	Средняя
п.4.5.5	Реализована возможность сохранения журналов аудита во внешние системы.		<- Выберите	**Высокая**
п.4.5.6	Журналы аудита Системы не содержат данных конфиденциального характера.		<- Выберите	**Высокая**
п.4.5.7	Журналы аудита Системы защищены от изменений.		<- Выберите	**Высокая**
п.4.5.8	**Сроки хранения журналов**	**Требования раздела неприменимы**	**0**	
п.4.5.8.1	Срок хранения журналов аудита в оперативном доступе в Системе составляет не менее трех месяцев.		<- Выберите	**Высокая**
п.4.5.8.2	По истечении установленного времени хранения журналов аудита в оперативном доступе они автоматически архивируются.		<- Выберите	Низкая
п.4.5.8.3	Срок хранения журналов аудита в архивном доступе составляет не менее одного года.		<- Выберите	**Высокая**
п.4.5.8.4	Журналы аудита имеют возможность автоматического разбиения и хранения по месяцам.		<- Выберите	Низкая
п.4.5.9	**Типы протоколируемых событий**	**Требования раздела неприменимы**	**0**	
п.4.5.9.1	Протоколируется работа пользователей с данными Системы (создание, чтение, изменение или удаление данных).		<- Выберите	Средняя

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.5.9.2	Протоколируются события аутентификации пользователя в Системе, в том числе неуспешные (включая окончание сессии).		<- Выберите	**Высокая**
п.4.5.9.3	Протоколируются действия привилегированных пользователей по настройке и изменению конфигурации Системы.		<- Выберите	**Высокая**
п.4.5.9.4	Протоколируется доступ к записям журнала протоколирования событий (включая их очистку).		<- Выберите	**Высокая**
п.4.5.9.5	Протоколируется запуск и остановка компонентов Системы.		<- Выберите	**Высокая**
п.4.5.10	**Протоколируемая инфомация**	**Требования раздела неприменимы**	**0**	
п.4.5.10.1	Протоколируется результат операции.		<- Выберите	**Высокая**
п.4.5.10.2	Протоколируется идентификатор источника операции.		<- Выберите	**Высокая**
п.4.5.10.3	Протоколируется идентификатор объекта, над которым была выполнена операция.		<- Выберите	**Высокая**
п.4.5.10.4	Протоколируется название и тип выполненной операции.		<- Выберите	Средняя
п.4.5.10.5	Протоколируется значение параметра до и после операции, если действие предполагает изменение данных или состояния компоненты Системы.		<- Выберите	Средняя
п.4.5.10.6	Протоколируется дата и время выполнения операции, включая указание часового пояса.		<- Выберите	**Высокая**
п.4.6	**Требования по отказоустойчивости**	**Требования раздела неприменимы**	**0**	
п.4.6.1	Реализована балансировка нагрузки между отдельными компонентами и модулями Системы.		<- Выберите	Низкая

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.6.2	Выстроены процессы резервного копирования и восстановления данных, обрабатываемых в Системе.		<- Выберите	Средняя
п.4.6.3	Процесс резервного копирования не работает с данными в монопольном режиме.		<- Выберите	Низкая
п.4.6.4	Резервная копия критичных данных шифруется.		<- Выберите	Низкая
п.4.7	**Требования к эксплуатации**	**Требования раздела неприменимы**	**0**	
п.4.7.1	По результатам аудита Системы со стороны ДИБ получено положительное заключение о возможности эксплуатации.		<- Выберите	**Высокая**
п.4.7.2	Реализовано поддержание актуальных версий компонентов Системы.		<- Выберите	**Высокая**
п.4.7.3	Обновления проходят тестирование перед установкой в продуктивной среде. Срок тестирования не превышает 1 месяца.		<- Выберите	Средняя
п.4.7.4	Организована техническая поддержка Системы с установленным SLA.		<- Выберите	Средняя
п.4.7.5	Разработка и тестирование изменений Системы не выполняются на продуктивных экземплярах Системы. На продуктивных экземплярах Системы не установлены средства разработки и тестирования.		<- Выберите	**Высокая**
п.4.7.6	Компоненты Системы обеспечены действующей технической поддержкой на ОС, СУБД, приложения и оборудование.		<- Выберите	Средняя
п.4.7.7	Все компоненты Системы зарегистрированы в корпоративных системах мониторинга и управления конфигурациями.		<- Выберите	**Высокая**

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.7.8	В продуктивной среде Системы отключен детальный вывод отладочной информации об ошибках, необходимой для разработки и отладки.		<- Выберите	**Высокая**
п.4.7.9	Для удаленного административного доступа к Системе и ее компонентам из корпоративной сети используются защищенные протоколы (SSH-2, SFTP, FTPS, SCP, RDP не ниже версии 6.0 и т.п.).		<- Выберите	**Высокая**
п.4.7.10	Пароли от предустановленных учетных записей в продуктивной Системе и ее компонентах изменены.		<- Выберите	**Высокая**
п.4.7.11	Доступ пользователей к Системе регламентируется локальными нормативными документами и предоставляется на основе заявок.		<- Выберите	**Высокая**
п.4.7.12	Административный доступ предоставлен только администраторам Системы.		<- Выберите	**Высокая**
п.4.7.13	На продуктивной Системе учетные записи разработчиков и / или производителей удалены или заблокированы.		<- Выберите	**Высокая**
п.4.10	**Требования к документации**	**Требования раздела неприменимы**	**0**	
п.4.10.1	Разработанные документы содержат описание системы.		<- Выберите	**Высокая**
п.4.10.2	Разработано руководство пользователя Системы (для внутренних пользователей).		<- Выберите	Низкая
п.4.10.3	Разработано руководство администратора Системы.		<- Выберите	Средняя
п.4.10.4	Разработана матрица доступа Системы.		<- Выберите	**Высокая**
п.4.10.5	Разработано регламент технического обслуживания.		<- Выберите	Низкая
п.4.10.6	Разработана схема резервного копирования данных.		<- Выберите	Средняя
п.4.10.7	Разработан регламент восстановления Системы при сбоях.		<- Выберите	Средняя

Пункт Стандарта	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.10.8	Документация доступна только авторизованным пользователям в рамках служебной необходимости. В документации отсутствует аутентификационная информация.		<- Выберите	**Высокая**
п.4.10.9	Исходные коды Системы не находятся в свободном доступе, если это не противоречит лицензии.		<- Выберите	**Высокая**
п.4.11	**Требования к ИСПДн**	**Требования раздела неприменимы**	**0**	
п.4.11.1	Система соответствует требованиям законодательства Российской Федерации в части обработки ПДн.		<- Выберите	**Высокая**
п.4.11.2	Система соответствует типовой модели угроз ПДн, утвержденной на Предприятии. Или разработана частная модель угроз, разработан и внедрен проект защиты ПДн Системы.		<- Выберите	**Высокая**
п.4.11.3	Обезличивание информации осуществляется в соответствии с приказом Роскомнадзора от 5 сентября 2013 г. № 996 и Методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденных руководителем Роскомнадзора 13.12.2013.		<- Выберите	**Высокая**
Итог	**Требования Стандарта**	**Не заполнено**	**0**	

Количество НЕвыполненных требований высокой критичности:	**0**	У
Количество НЕвыполненных требований средней критичности:	**0**	У

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.1	**Требования к HTTP-заголовкам**	**Требования раздела неприменимы**	**0**	
п.1.1	Используется заголовок «Strict-Transport-Security» Значение «max-age» не менее 31536000.		<- Выберите	**Высокая**
п.1.2	Используется заголовок «X-Frame-Options». Параметр «X-Frame-Options» имеет значение «deny» или «sameorigin».		<- Выберите	**Высокая**
п.1.3	Используется заголовок «X-XSS-Protection: 1». Установлен параметр «mode=block».		<- Выберите	**Высокая**
п.1.4	Используется заголовок «X-Content-Type-Options: nosniff».		<- Выберите	**Высокая**
п.1.5	Используется заголовок «Referrer-Policy». Параметр «Referrer-Policy» имеет значение «no-referrer» или «same-origin».		<- Выберите	**Высокая**
п.1.6	Используется заголовок «Feature-Policy». Для функций «camera», «geolocation», «microphone», «payment», «speaker», «vibrate» и «usb» заданы значения.		<- Выберите	Средняя
п.1.7	**Заголовок «Content-Security-Policy»**	**Требования раздела неприменимы**	**0**	
п.1.7.1	В «Content-Security-Policy» задана директива «default-src».		<- Выберите	Средняя
п.1.7.2	В «Content-Security-Policy» задана директива «script-src».		<- Выберите	Средняя
п.1.7.3	В «Content-Security-Policy» задана директива «style-src».		<- Выберите	Средняя

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.1.7.4	В «Content-Security-Policy» заданы директивы источников других объектов (изображения, аудио, видео, шрифты и др.).		<- Выберите	Средняя
п.1.7.5	В «Content-Security-Policy» задан параметр «report-uri».		<- Выберите	Низкая
п.1.7.6	В «Content-Security-Policy» соблюдены требования к параметру «nonce».		<- Выберите	Средняя
п.1.7.7	В «Content-Security-Policy» соблюдены требования к параметру «hash».		<- Выберите	Средняя
п.1.7.8	В «Content-Security-Policy» соблюдены требования к параметру «'unsafe-inline'».		<- Выберите	Средняя
п.1.7.9	В «Content-Security-Policy» соблюдены требования к параметру «'unsafe-eval'».		<- Выберите	Средняя
п.2	**Требования к активному содержимому и скриптам**	**Требования раздела неприменимы**	**0**	
п.2.1	Исходный код скриптов и активных компонент, исполняемых на клиентской стороне, не содержит сведений конфиденциального характера.		<- Выберите	**Высокая**
п.2.2	Технологии AJAX не используются для обработки платежной информации.		<- Выберите	**Высокая**
п.2.3	**Требования к сценариям JavaScript**	**Требования раздела неприменимы**	**0**	
п.2.3.1	Сценарии JavaScript не обрабатывают структуры и данные, обеспечивающие безопасность web-приложения.		<- Выберите	**Высокая**
п.2.3.2	В web-приложении используются только JavaScript-сценарии из системы хранения исходного кода Предприятия.		<- Выберите	Низкая

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.2.4	**Требования к ActiveX и сценариям Visual Basic**	**Требования раздела неприменимы**	**0**	
п.2.4.1	Скрипты, написанные на Visual Basic, не используются.		<- Выберите	**Высокая**
п.2.4.2	Компоненты ActiveX не используются.		<- Выберите	Низкая
п.2.5	**Требования к Java-апплетам**	**Требования раздела неприменимы**	**0**	
п.2.5.2	Все используемые Java-апплеты имеют цифровую подпись доверенного удостоверяющего центра.		<- Выберите	**Высокая**
п.2.5.3	В коде апплета не используются механизмы принятия критичных решений (например, относящимся к механизмам безопасности или бизнес процессам).		<- Выберите	**Высокая**
п.2.5.4	Используется обфускация байт-кода Java-апплетов.		<- Выберите	Низкая
п.3	**Требования к проверке входных и выходных параметров**	**Требования раздела неприменимы**	**0**	
п.3.1	Все входные параметры проверяются на серверной стороне.		<- Выберите	**Высокая**
п.3.2	Проверка входных параметров осуществляется до их использования компонентами web-приложения.		<- Выберите	**Высокая**
п.3.3	Web-приложение проверяет полноту полученных от пользователя параметров.		<- Выберите	**Высокая**
п.3.4	HTTP-заголовки и скрытые HTML-поля (<input type=hidden>) проходят проверку, как и обычные HTTP-параметры.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.3.5	Сообщения об ошибках не содержат сведений, по которым возможно восстановить метод проверки параметров.		<- Выберите	**Высокая**
п.3.6	Осуществляется дополнительная проверка входных параметров от пользователя в клиентской части web-приложения.		<- Выберите	Низкая
п.3.7	**Очистка возвращаемых данных**	**Требования раздела неприменимы**	**0**	
п.3.7.1	Проверка возвращаемых пользователю данных осуществляется до момента отправки web-страницы от сервера браузеру.		<- Выберите	Средняя
п.3.7.2	Форматирование выводимой пользователю HTML-разметки осуществляется средствами CMS или доверенных библиотек.		<- Выберите	Низкая
п.3.7.3	В случае необходимости визуализации управляющих символов серверная часть web-приложения должна осуществлять их замену на «видимые» аналоги.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4	**Предотвращение раскрытия информации**	**Требования раздела неприменимы**	**0**	
п.4.1	Аутентификационная информация передается по защищенному протоколу TLS.		<- Выберите	**Высокая**
п.4.2	**Минимизация вывода информации**	**Требования раздела неприменимы**	**0**	
п.4.2.1	Исходный код web-страниц не содержит служебную информацию.		<- Выберите	**Высокая**
п.4.2.2	Сообщения об ошибках не содержат информации о версии программного обеспечения, внутренних путей, а также ранее введенных пользователем данных.		<- Выберите	**Высокая**
п.4.2.3	Компоненты Системы сконфигурированы таким образом, чтобы затруднить атакующему определение их реальных версий.		<- Выберите	Средняя
п.4.3	**Требования к формированию URL**	**Требования раздела неприменимы**	**0**	
п.4.3.1	URL не содержат сведений конфиденциального характера.		<- Выберите	**Высокая**
п.4.3.2	Передача конфиденциальных данных осуществляется с помощью метода «POST».		<- Выберите	**Высокая**
п.4.3.3	Web-приложение не использует «секретных» HTTP-параметров для перехода в режим отладки, администрирования или получения доступа к неподдерживаемому в обычном режиме функционалу.		<- Выберите	**Высокая**
п.4.3.4	Конфиденциальные данные не передаются в рамках перенаправления (редиректа) на другие web-ресурсы.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.5	**Требования к сессиям**	**Требования раздела неприменимы**	**0**	
п.5.1	**Требования к идентификаторам сессий (Session ID)**	**Требования раздела неприменимы**	**0**	
п.5.1.1	Идентификатор сессии уникальный и не предугадываемый.		<- Выберите	**Высокая**
п.5.1.2	Идентификатор сессии устойчив к подбору. Длина идентификатора сессии превышает 128 бит.		<- Выберите	**Высокая**
п.5.1.3	Идентификатор сессии не зависит от других идентификаторов (сформированных ранее), имени пользователя, пароля, состояния приложения.		<- Выберите	**Высокая**
п.5.1.4	Клиентская часть web-приложения не имеет возможности изменять идентификатор сессии.		<- Выберите	**Высокая**
п.5.1.5	В случае, когда web-приложение использует TLS для передачи данных, идентификатор сессии всегда передается внутри защищенного соединения.		<- Выберите	Средняя
п.5.1.6	Новый идентификатор сессии формируется приложением каждый раз после прохождения успешной аутентификации пользователя.		<- Выберите	**Высокая**
п.5.2	**Управление сессиями**	**Требования раздела неприменимы**	**0**	
п.5.2.1	Время жизни сессий ограничено. По истечении данного времени, сессия удаляется или генерируется новый запрос на обновление аутентификации.		<- Выберите	**Высокая**
п.5.2.2	Неактивные сессии завершаются автоматически.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.5.2.3	Web-приложение на клиентской стороне не поддерживает сессию в активном состоянии искусственно.		<- Выберите	**Высокая**
п.5.2.4	Используются встроенные в стандартные библиотеки и механизмы управления сессиями.		<- Выберите	Низкая
п.5.2.5	Данные о сессиях пользователей хранятся в месте, не доступном для других приложений и систем (в том случае, если они не защищены другим способом, например, путем шифрования).		<- Выберите	**Высокая**
п.5.2.6	Для доступа к ПДн или совершения транзакций требуется прохождение стандартной процедуры аутентификации и проверки прав.		<- Выберите	**Высокая**
п.5.2.7	Возможность использования механизма автоматической аутентификации («запомнить меня») доступна только для некритичных действий.		<- Выберите	**Высокая**
п.5.3	**Завершение сессий**	**Требования раздела неприменимы**	**0**	
п.5.3.1	Web-приложение содержит механизм завершения сессии, доступный пользователю из любой страницы приложения.		<- Выберите	**Высокая**
п.5.3.2	По завершении сессии относящиеся к ней конфиденциальные данные полностью удаляются на серверной стороне.		<- Выберите	**Высокая**
п.5.3.3	Сессия, содержащая конфиденциальные данные, автоматически завершается при закрытии браузера.		<- Выберите	**Высокая**
п.5.3.4	По завершении сессии ее данные на ПК клиента удаляются.		<- Выберите	Низкая

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.6	**Требования к использованию протокола HTTP**	**Требования раздела неприменимы**	**0**	
п.6.1	Для передачи сведений, составляющих коммерческую тайну и иную конфиденциальную информацию, используется протокол HTTPS.		<- Выберите	**Высокая**
п.6.2	Web-приложение поддерживает минимально необходимый набор HTTP-методов.		<- Выберите	**Высокая**
п.6.3	**Требования к использованию cookies**	**Требования раздела неприменимы**	**0**	
п.6.3.1	Атрибут «HTTPOnly» для cookies имеет значение «true».		<- Выберите	**Высокая**
п.6.3.2	Если используется протокол HTTPS, для cookies установлен флаг «secure».		<- Выберите	**Высокая**
п.6.3.3	Атрибут cookies «domain» установлен значением только того ресурса, для которого требуется поддержка данного cookie.		<- Выберите	**Высокая**
п.6.3.4	Атрибут cookies «path» настроен таким образом, чтобы браузер пользователя отправлял cookies только тому web-приложению, которому они предназначаются.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.7	**Требования к HTML**	**Требования раздела неприменимы**	**0**	
п.7.1	**Требования к комментариям и скрытым полям HTML**	**Требования раздела неприменимы**	**0**	
п.7.1.1	HTML-комментарии не содержат внутреннюю информацию web-приложения а также не раскрывают особенности реализации Системы.		<- Выберите	**Высокая**
п.7.1.2	В скрытых полях HTML-страниц в незашифрованном виде не передаются конфиденциальные сведения, аутентификационная информация, а также управляющие команды.		<- Выберите	**Высокая**
п.7.2	**Требования к всплывающим окнам (pop-up)**	**Требования раздела неприменимы**	**0**	
п.7.2.1	Всплывающие окна используются только для отображения информационных сообщений.		<- Выберите	**Высокая**
п.7.2.2	Всплывающие окна не используются для получения данных от пользователя.		<- Выберите	**Высокая**
п.8	**Криптография**	**Требования раздела неприменимы**	**0**	
п.8.1	В качестве криптографического протокола используется TLS не ниже v.1.2.		<- Выберите	**Высокая**
п.8.2	В случае перенаправления пользователя с защищенных ресурсов web-приложения на незащищенные сессия клиента либо завершается либо удаляются конфиденциальные данные, использовавшиеся в рамках сессии.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.8.3	Конфиденциальная информация передается только по защищенному протоколу HTTPS.		<- Выберите	**Высокая**
п.8.4	Использование гиперссылок, перенаправляющих с защищенных web-страниц приложения на незащищенные, не приводит к появлению конфиденциальных сведений в поле «HTTP-referer».		<- Выберите	**Высокая**
п.9	**Требования к архитектуре**	**Требования раздела неприменимы**	**0**	
п.9.1	Форма регистрации клиентов в web-приложении защищена от автоматических средств регистрации (ботов).		<- Выберите	**Высокая**
п.9.2	**Требования к контролю состояний процессов**	**Требования раздела неприменимы**	**0**	
п.9.2.1	Web-приложение контролирует состояние процесса, на котором находится клиент.		<- Выберите	**Высокая**
п.9.2.2	Механизм контроля состояний процессов реализован на серверной стороне web-приложения.		<- Выберите	Низкая
п.9.2.3	Индикатор состояния процесса уникальный и не предугадываемый.		<- Выберите	**Высокая**
п.9.2.4	Содержимое HTTP-referer не используется для контроля состояния процессов.		<- Выберите	**Высокая**
п.9.3	**Скрытые и замаскированные ресурсы**	**Требования раздела неприменимы**	**0**	
п.9.3.1	Все страницы и активные скрипты web-сервера, к которым пользователь может получить доступ, являются частью web-приложения.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.9.3.2	Доступ к файлам не ограничивается путем переименования файлов или путем не указания гиперссылок на них.		<- Выберите	**Высокая**
п.9.3.3	Неиспользуемые директории и файлы на продуктивном сервере отсутствуют.		<- Выберите	**Высокая**
п.9.4	**Требования к аутентификации**	**Требования раздела неприменимы**	**0**	
п.9.4.1	Учетные данные не хранятся в местах, доступных для клиента.		<- Выберите	**Высокая**
п.9.4.2	Процесс аутентификации не основывается на данных и переменных, которые можно легко модифицировать.		<- Выберите	**Высокая**
п.9.4.3	При начальной регистрации пользователя или восстановлении утерянного пароля предусмотрена проверка его сложности.		<- Выберите	Средняя
п.9.4.4	Для доступа к разделам, связанным с пользовательской информацией и выполнением действий от лица пользователя, требуется обязательная аутентификация.		<- Выберите	Средняя
п.9.4.5	Процедура аутентификации имеет защиту от подбора паролей.		<- Выберите	**Высокая**
п.9.5	**Требования к авторизации**	**Требования раздела неприменимы**	**0**	
п.9.5.1	Web-сервер запущен под специально созданной технологической учетной записью ОС с минимально необходимым набором привилегий.		<- Выберите	Средняя

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.9.5.2	Учетной записи СУБД, под которым работает web-приложение, предоставлены ограниченные права на работу с файловой системой сервера, а также на исполнение команд ОС.		<- Выберите	**Высокая**
п.9.6	**Взаимодействие между компонентами**	**Требования раздела неприменимы**	**0**	
п.9.6.1	При обращении к базам данных web-приложение использует хранимые процедуры вместо SQL-запросов, содержащих параметры.		<- Выберите	**Высокая**
п.9.6.2	Хранение паролей в БД web-приложения осуществляется с использованием криптографических алгоритмов, определяемых в соответствии с пунктом 4.1.1 Стандарта.		<- Выберите	**Высокая**
п.9.6.3	Доступ к web-интерфейсам администрирования web-приложений из сети интернет запрещен.		<- Выберите	**Высокая**
п.9.6.4	Административные и пользовательские интерфейсы разделены. Пользовательский интерфейс не предоставляет возможностей администрирования Системы.		<- Выберите	**Высокая**
п.9.6.5	Web-интерфейсы систем мониторинга не доступны из сети интернет.		<- Выберите	**Высокая**
п.9.7	**Контроль состояния клиента**	**Требования раздела неприменимы**	**0**	
п.9.7.1	Используется механизм контроля состояния клиента, путем присвоения клиенту начального идентификатора состояния и его последовательного изменения в процессе работы.		<- Выберите	Средняя

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.9.7.2	Если механизм управления состоянием используется на стороне клиента, параметр контроля состояния клиента шифруется.		<- Выберите	**Высокая**
п.9.8	**Сокрытие внутренней структуры**	**Требования раздела неприменимы**	**0**	
п.9.8.1	Не используется прямое, легко угадываемое именование содержимого.		<- Выберите	**Высокая**
п.9.8.2	Контролируется отсутствие информации о внутренней структуре Системы или сети Предприятия в ответах и страницах web-приложений Системы.		<- Выберите	**Высокая**
п.10	**Требования к API**	**Требования раздела неприменимы**	**0**	
п.10.1	Структура запросов к API задокументирована.		<- Выберите	**Высокая**
п.10.2	Для каждой функции реализована авторизация.		<- Выберите	**Высокая**
п.10.3	Количество субъектов, данные по которым отдаются в одном ответе, ограничено.		<- Выберите	Низкая
п.10.4	Система отдает по API только те данные, которые были запрошены.		<- Выберите	**Высокая**
п.10.5	**Требования к «секрету»**	**Требования раздела неприменимы**	**0**	
п.10.5.1	Для аутентификации подключаемых систем используется «секрет».		<- Выберите	**Высокая**
п.10.5.2	«Секрет» не внедрен в код системы.		<- Выберите	**Высокая**

Пункт Прил.2	Требования (вопрос)	Выполнение	Баллы	Критичность
п.10.5.3	«Секрет» доступен только для использования конкретной системой-клиентом (привязка по IP).		<- Выберите	Средняя
п.10.5.4	Срок действия «секрета» не превышет 1 года.		<- Выберите	Средняя
Итог	**Требования Приложения 2 к Стандарту**	**Не заполнено**	**0**	

Количество НЕвыполненных требований высокой критичности:	**0**	У
Количество НЕвыполненных требований средней критичности:	**0**	У

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.2	**Хранение данных и конфиденциальность**	**Требования раздела неприменимы**	**0**	
п.2.1	**Работа с ключами шифрования**	**Требования раздела неприменимы**	**0**	
п.2.1.1	Используемые в приложении ключи шифрования хранятся в системном хранилище ключей.		<- Выберите	**Высокая**
п.2.1.2	Приложение не содержит ключи шифрования в исходном коде.		<- Выберите	**Высокая**
п.2.1.3	Приложение использует ключи шифрования длины не менее: 256 бит – для симметричных шифров, 3072 бит – для асимметричных.		<- Выберите	**Высокая**
п.2.1.4	Приложение не использует один и тот же ключ шифрования для нескольких целей.		<- Выберите	**Высокая**
п.2.2	**Обработка конфиденциальной информации**	**Требования раздела неприменимы**	**0**	
п.2.2.1	КИ хранится во внутреннем хранилище приложения либо в защищенном системном хранилище данных.		<- Выберите	**Высокая**
п.2.2.2	Продуктивная версия приложения не сохраняет КИ в журнал сбора событий.		<- Выберите	**Высокая**
п.2.2.3	Приложение не хранит КИ в памяти дольше, чем это требуется.		<- Выберите	Средняя
п.2.2.4	Приложение удаляет КИ из оперативной памяти сразу после окончания работы с ней.		<- Выберите	Средняя
п.2.2.5	КИ не передается через механизмы IPC.		<- Выберите	Средняя

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.2.2.6	**Отображение КИ на экране устройства**	**Требования раздела неприменимы**	**0**	
п.2.2.6.1	КИ, такая как пароли или пин-код, не отображается в пользовательском интерфейсе (если не предусмотрено дро.функционалом).		<- Выберите	**Высокая**
п.2.2.6.2	Приложение не содержит КИ на экране быстрого доступа.		<- Выберите	Средняя
п.2.2.6.3	Небезопасные уведомления не содержат КИ.		<- Выберите	**Высокая**
п.2.2.7	**КИ в текстовых полях**	**Требования раздела неприменимы**	**0**	
п.2.2.7.1	Кэш клавиатуры отключен для текстовых полей, которые могут содержать КИ.		<- Выберите	**Высокая**
п.2.2.7.2	Буфер обмена отключен для текстовых полей, которые могут содержать КИ.		<- Выберите	**Высокая**
п.3	**Криптография**	**Требования раздела неприменимы**	**0**	
п.3.1	Приложение использует только проверенные реализации криптографических алгоритмов (Приложение 3 Стандарта).		<- Выберите	**Высокая**
п.3.2	Приложение явно определяет режим (параметры, технологии) шифрования.		<- Выберите	**Высокая**
п.3.3	Приложение использует случайные числа, сгенерированные с использованием встроенных функций операционной системы.		<- Выберите	Средняя
п.3.4	Ключи шифрования не хранятся в исходном коде.		<- Выберите	**Высокая**

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.3.5	**Сетевые соединения**	**Требования раздела неприменимы**	**0**	
п.3.5.1	Канал связи защищен с помощью TLS не ниже v.1.2.		<- Выберите	**Высокая**
п.3.5.2	Приложение использует актуальные версии библиотек для организации безопасности и установки соединений.		<- Выберите	**Высокая**
п.3.6	**Требования к работе с сертификатами**	**Требования раздела неприменимы**	**0**	
п.3.6.1	Перед установкой TLS-соединения приложение проверяет сертификат сервера, с которым устанавливается соединение.		<- Выберите	**Высокая**
п.3.6.2	Приложение проверяет, что срок действия и другие свойства сертификата сервера действительны.		<- Выберите	**Высокая**
п.3.6.3	Приложение проверяет, что имя сервера системы соответствует CN (Common Name) или SAN (альтернативные имена объектов) в поле «Subject» сертификата сервера.		<- Выберите	Средняя
п.3.6.4	Приложение использует свое собственное хранилище сертификатов или механизм SSL Pinning.		<- Выберите	Средняя
п.3.6.5	Используемые приложением сертификаты не хранятся в общедоступных местах.		<- Выберите	**Высокая**
п.4	**Аутентификация**	**Требования раздела неприменимы**	**0**	
п.4.1	Для входа в приложение должна использоваться аутентификация.		<- Выберите	**Высокая**
п.4.2	Сервер предоставляет токен, подписанный с использованием криптографически стойкого алгоритма шифрования (см. Приложение 3 Стандарта).		<- Выберите	**Высокая**

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.4.3	При аутентификации с помощью биометрической информации событие успешной проверки отпечатка используется для разблокировки ключа в хранилище ключей, а не для входа в систему.		<- Выберите	Средняя
п.4.4	В приложении настроена парольная политика, параметры которой устанавливаются на сервере.		<- Выберите	**Высокая**
п.4.5	Для критичных операций запрашивается дополнительное подтверждение или повторная аутентификация.		<- Выберите	Низкая
п.4.6	Приложение предоставляет пользователю информацию о нескольких последних входах в систему и список использовавшихся для входа устройств.		<- Выберите	Низкая
п.4.7	В Приложении реализована возможность применения второго фактора аутентификации.		<- Выберите	Низкая
п.5	**Управление сессиями**	**Требования раздела неприменимы**	**0**	
п.5.1	Идентификатор сессии генерируется случайным образом.		<- Выберите	**Высокая**
п.5.2	При создании идентификатора сессии используется генератор случайных чисел (см. П3.3.3).		<- Выберите	Средняя
п.5.3	При выходе пользователя из приложения сессия закрывается (инвалидируется).		<- Выберите	Средняя
п.5.4	По истечении заданного срока неактивности пользователя или срока действия токена сессия закрывается (инвалидируется) приложением.		<- Выберите	**Высокая**

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.6	**Взаимодействие с платформой**	**Требования раздела неприменимы**	**0**	
п.6.1	Приложение запрашивает минимально необходимый набор разрешений.		<- Выберите	**Высокая**
п.6.2	Приложение обеспечивает применение ограничений для доступа к устройству.		<- Выберите	Средняя
п.6.3	Приложение валидирует и санитизирует все входные данные из внешних источников и от пользователя на устройстве.		<- Выберите	Средняя
п.6.4	Отключена возможность создания резервной копии приложения или резервная копия не должна содержать КИ.		<- Выберите	**Высокая**
п.6.5	**Дополнительные требования к объекту «WebView»**	**Требования раздела неприменимы**	**0**	
п.6.5.1	В элементе «WebView» разрешен только обработчик протокола HTTPS.		<- Выберите	**Высокая**
п.6.5.2	Приложение не игнорирует ошибки SSL в WebView.		<- Выберите	**Высокая**
п.6.5.3	Приложение загружает JavaScript для WebView только из ресурсов приложения.		<- Выберите	**Высокая**
п.6.5.4	JavaScript отключен в WebView.		<- Выберите	**Высокая**
п.7	**Качество клиентского кода**	**Требования раздела неприменимы**	**0**	
п.7.1	Исходные коды приложения проверены на отсутствие актуальных угроз безопасности мобильным приложениям.		<- Выберите	**Высокая**
п.7.2	Продуктивная версия подписана действующим сертификатом.		<- Выберите	**Высокая**

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.7.3	Продуктивная версия приложения скомпилирована в режиме «release». Установлены параметры для продуктивных приложений.		<- Выберите	**Высокая**
п.7.4	Отладочная информация удалена из бинарных файлов приложения.		<- Выберите	**Высокая**
п.7.5	Приложение перехватывает и обрабатывает возможные исключения.		<- Выберите	**Высокая**
п.7.6	Приложение не записывает и не хранит подробные сведения об ошибке и отладочные сообщения в штатном режиме работы.		<- Выберите	Низкая
п.7.7	Все используемые компоненты приложения проверены на наличие уязвимостей.		<- Выберите	**Высокая**
п.7.8	В случае сбоя в работе функции предоставления доступа по умолчанию доступ не предоставляется.		<- Выберите	**Высокая**
п.7.9	Активированы все стандартные функции безопасности, предусмотренные инструментами разработчика.		<- Выберите	**Высокая**
п.8	**Противодействие атакам**	**Требования раздела неприменимы**	**0**	
п.8.1	Приложение реализует привязку к устройству.		<- Выберите	Средняя
п.8.2	**Требования к обнаружению атак**	**Требования раздела неприменимы**	**0**	
п.8.2.1	Приложение определяет наличие root или jailbreak на устройстве.		<- Выберите	**Высокая**
п.8.2.2	Приложение определяет работу под отладчиком.		<- Выберите	Средняя
п.8.2.3	Приложение определяет установленные на устройстве приложения для reverse engineering.		<- Выберите	Средняя
п.8.2.4	Приложение определяет работу на эмуляторе.		<- Выберите	Средняя

Пункт Прил. 3	Требования (вопрос)	Выполнение	Баллы	Критичность
п.8.2.5	Приложение определяет изменение исполняемых файлов и критичных данных в своей песочнице (своем окружении).		<- Выберите	**Высокая**
п.8.2.6	Приложение определяет изменение своего кода или данных в оперативной памяти.		<- Выберите	**Высокая**
п.8.3	**Требования к обфускации**	**Требования раздела неприменимы**	**0**	
п.8.3.1	В приложении используется обфускация.		<- Выберите	**Высокая**
п.8.3.2	Задачей обфускации является защита вычислений, используется механизм, который: - применим для этой задачи; - защищает от ручной и автоматической де-обфускации; - учитывает опубликованные по этой теме исследования.		<- Выберите	**Высокая**
п.9	**Требования к приложениям для Android**	**Требования раздела неприменимы**	**0**	
п.9.1	При запуске Activity в идентификатор (URI), устанавливаемый в методе «Intent#setData()», не включается КИ.		<- Выберите	**Высокая**
п.9.2	Все компоненты приложения, которые используются только внутри приложения, являются «Private».		<- Выберите	Средняя
п.9.3	Для запуска всех компонентов приложения Private, Partner или In-house используется явный Intent.		<- Выберите	**Высокая**
Итого	**Требования Приложения 3 к Стандарту**	**Не заполнено**	**0**	

Количество НЕвыполненных требований высокой критичности:	**0**	У
Количество НЕвыполненных требований средней критичности:	**0**	У