

ПРИКАЗ

18.05.2020 № 141-н

МОСКВА

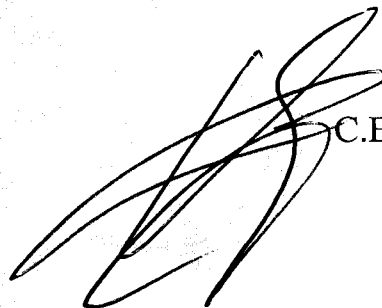
[Об утверждении Стандарта
«Обеспечение информационной
безопасности при разработке
или модернизации плагинов
ЕАС ОПС АО «Почта России»]

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 плагинов ЕАС ОПС АО «Почта России».

2. Признать утратившим силу Стандарт «Обеспечение информационной безопасности при разработке или модернизации плагинов ЕАС ОПС ФГУП «Почта России», утвержденный 16.05.2017 № 1.9.3.1.2-05/54-нд.

Заместитель генерального директора
по информационным технологиям
и развитию цифровых сервисов

 С.Е. Емельченков

Приложение

УТВЕРЖДЕНО

приказом АО «Почта России»

от 18.05.2020 № 141-н

СТАНДАРТ

«Обеспечение информационной безопасности при разработке или
модернизации плагинов ЕАС ОПС АО «Почта России»

Москва, 2020

Оглавление

1. Термины и определения.....	3
2. Основные положения	5
3. Организационные требования.....	6
4. Требования к разрабатываемым или модернизируемым плагинам	6
Приложение к Стандарту	12

1. Термины и определения

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

Наименование термина	Сокращение	Определение термина
Внешний интерфейс		сервис, через который осуществляется непосредственное взаимодействие с внешними пользователями
Внутренний интерфейс		сервис, через который осуществляется непосредственное взаимодействие с внутренними пользователями и/или администраторами
Департамент информационной безопасности		Департамент информационной безопасности Блока по корпоративной безопасности АО «Почта России»
Единая автоматизированная информационная система отделения почтовой связи	ЕАС ОПС	Единая автоматизированная информационная система отделения почтовой связи АО «Почта России»
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 характеризующееся способностью обеспечивать конфиденциальность, целостность и доступность информации при ее хранении, обработке и передаче на заданном владельцем уровне
Информационная система		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
Компонент системы		компонентом системы является любое сетевое устройство, сервер или приложение, входящее в состав информационной системы или подключенное к среде передачи данных
Минимально необходимые права доступа		набор прав доступа в информационные системы, позволяющих выполнять в информационных системах операции, определяемые должностными обязанностями работника, и не превышающие их
Модель угроз		документ, в котором определяются актуальные для Системы угрозы информационной безопасности
Несанкционированный доступ		нарушение регламентированного порядка доступа к объекту защиты

Наименование термина	Сокращение	Определение термина
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 прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)
Плагин (англ. plug-in)		независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и/или использования ее возможностей
Система		прикладные системы и приложения, используемые в АО «Почта России»
Система управления базами данных	СУБД	совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных
Пользователь		лицо, участвующее в функционировании информационной системы
Права доступа пользователя		совокупность правил, регламентирующих порядок и условия доступа пользователя к информации и ее носителям, установленных нормативными документами или владельцем информационного актива (ресурса)
Общество		АО «Почта России»
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 информационной системе
Active Directory	AD	Служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
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.
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

Наименование термина	Сокращение	Определение термина
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
SSH File Transfer Protocol	SFTP	протокол, предназначенный для обмена и управления данными поверх какого-либо криптографического протокола (обычно SSH)
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
Virtual Private Network	VPN	виртуальная частная сеть. Логическая сеть, создаваемая поверх другой сети, и используемая для безопасной пересылки данных
Web-приложение		клиент-серверная Система, в которой клиентом выступает браузер, а сервером – веб-сервер

2. Основные положения

Настоящий Стандарт разработан с целью унификации требований по информационной безопасности, предъявляемых к новым или модернизируемым плагинам ЕАС ОПС Общества (далее – плагины), обеспечения конфиденциальности, целостности и доступности обрабатываемой в них информации с учетом исполнения требований законодательства Российской Федерации, семейства стандартов ISO/IEC 27000, локальных нормативных актов Общества.

В случае необходимости доработки ЕАС ОПС или Систем, с которыми взаимодействует плагин, к вышеуказанным Системам дополнительно предъявляются требования информационной безопасности, определенные Стандартом «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений АО «Почта России», утвержденным приказом Общества от 16.01.2020 № 7-п (далее – Стандарт 1).

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

Подразделением, ответственным за координацию и контроль исполнения настоящего Стандарта, является Департамент информационной безопасности.

Отступление от требований настоящего Стандарта осуществляется по согласованию с Департаментом информационной безопасности.

Настоящий Стандарт подлежит пересмотру и актуализации (в случае необходимости) не реже 1 раза в три года, а также в случае изменения законодательства в области информационной безопасности, касающегося положений Стандарта.

Актуальная версия Стандарта размещается на корпоративном портале.

3. Организационные требования

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

3.2. Работники Департамента информационной безопасности должны включаться в состав комиссии (проектной команды) по разработке или модернизации плагина.

3.3. Требования настоящего Стандарта должны в обязательном порядке включаться в технические задания на разработку или модернизацию плагина.

3.4. Ввод плагина в эксплуатацию (опытную/промышленную) возможен после успешного прохождения испытаний плагина и получения положительного заключения о его соответствии требованиям информационной безопасности. Перед сдачей плагина в Департамент информационной безопасности на прохождение испытаний должно быть представлено Описание реализации требований Стандарта (шаблон приведен в приложении к Стандарту).

4. Требования к разрабатываемым или модернизируемым плагинам

4.1. Общие требования

4.1.1. Должна осуществляться проверка/валидация любых входных данных на длину, допустимые символы, кодировку, полноту данных (наличие обязательных параметров). Проверка должна осуществляться до процесса их обработки в плагине и передачи во внешние компоненты.

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

4.2. Требования к аутентификации и авторизации

4.2.1. Доступ к функционалу плагина должен предоставляться только после успешного прохождения процесса аутентификации пользователя и последующей его авторизации. Все действия в плагинах должны производиться с использованием учетных записей, наделенных минимально необходимыми привилегиями.

4.2.2. Прохождение аутентификации пользователя возможно либо в ЕАС ОПС либо в Системе, с которой взаимодействует плагин.

4.2.3. Для прозрачной аутентификации пользовательские пароли допускается хранить в локальной базе ЕАС ОПС. Доступ к локальной базе ЕАС ОПС должен осуществляться под учетной записью с минимальными правами. Пароли в локальной базе ЕАС ОПС должны храниться только в

зашифрованном виде. Должны использоваться стойкие криптографические алгоритмы или алгоритмы хеширования. Перечень криптографически стойких алгоритмов (далее – Перечень) утверждается заместителем генерального директора по корпоративной безопасности Общества и размещается на корпоративном портале. Запрещается использовать репликацию парольной информации из локальной базы ЕАС ОПС на все рабочие станции ЕАС ОПС.

4.2.4. В случае взаимодействия плагина с Системами, где предъявляются повышенные требования к обеспечению информационной безопасности, (например, при передаче по сети финансовых операций), должна осуществляться процедура взаимной аутентификации, например, на основе проверки пользовательского сертификата.

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

- пользовательские сертификаты;
- пароли;
- средства двухфакторной аутентификации (USB-токен, смарт-карта и т.п.);
- средства биометрической аутентификации.

4.2.6. Для каждого пользователя необходимо использовать следующие основные атрибуты безопасности: идентификатор пользователя (логин, табельный номер и т.п.), аутентификационная информация (например, пароль), права доступ к объекту защиты (роль).

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

4.2.8. Использование групповых учетных записей запрещено.

4.2.9. В компонентах плагина должны отсутствовать жестко запрограммированные учетные записи.

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

4.2.11. Подсистема аутентификации плагина должна обеспечивать возможность настройки парольной политики в части:

- самостоятельной смены пароля пользователем при первом входе в плагин, а также в любое время по его усмотрению;
- отключения администратором функции смены паролей у отдельных пользователей;
- установки парольной политики для всех пользователей, группы пользователей или отдельно для каждой учетной записи в соответствии с локальными нормативными актами Общества;
- принудительной смены пароля пользователем через установленный промежуток времени;

- заблаговременного оповещения пользователей о необходимости смены пароля (посредством сообщений/подсказок или почтовых рассылок на электронные адреса пользователей);
- блокировки учетной записи на заранее определенный срок после заданного количества неудачных попыток аутентификации;
- установки срока длительности простоя пользовательской сессии, после которого сессия должна принудительно завершаться;
- ограничения множественного входа в систему под одной учетной записью пользователя.

Дополнительно для внутренних пользователей подсистема аутентификации должна осуществлять:

- автоматическую блокировку учетной записи пользователя, в случае если пароль не был изменен до установленной даты;
- хранение истории паролей пользователей, как минимум за последние 12 месяцев для предотвращения повторного их использования.

4.2.12. Восстановление пароля должно производиться только путем его смены.

4.2.13. В процессе аутентификации проверка введенной информации (логина и пароля) должна осуществляется только после полного ее ввода. В случае обнаружения ошибки, плагин не должен выдавать сообщение, какие именно данные введены неправильно. Пароль не должен отображаться при вводе.

4.2.14. Доступ к функционалу плагина может подразделяться на пользовательский и административный и должен быть реализован на основе ролей с учетом принципов разделения обязанностей и минимизации полномочий. Должно быть предусмотрено наличие средств управления ролями плагина: создание новых, редактирование, удаление.

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

4.3. Требования к криптографической защите при передаче данных

4.3.1. Конфиденциальные данные, хранящиеся локально в ЕАС ОПС или передающиеся по сетям общего пользования, должны быть защищены с использованием криптографически стойких алгоритмов шифрования из утвержденного в Обществе Перечня.

4.3.2. Информация ограниченного доступа, обеспечение конфиденциальности которой определяется законодательством Российской Федерации, при передаче по сетям общего пользования должна защищаться с использованием средств криптографической защиты информации, имеющих сертификат соответствия ФСБ России.

4.3.3. В качестве альтернативного решения для защиты передачи данных по сетям общего пользования можно применять обезличивание информации в соответствии с приказом Роскомнадзора от 05.09.2013 № 996

"Об утверждении требований и методов по обезличиванию персональных данных" и методическими рекомендациями к нему.

4.3.4. Сетевой обмен по сетям общего пользования информацией, обеспечение конфиденциальности которой не определяется законодательством Российской Федерации, 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, STP, L2TP и т.д.).

4.4. Требования к окружению

4.4.1. Разрабатываемые или модернизируемые плагины должны корректно функционировать с используемыми в Обществе:

- средствами обеспечения безопасности рабочих станций и серверов, например, антивирусами, средствами контроля внешних устройств, средствами криптографической защиты информации и т.д.;

- ОС, СУБД, прикладными программами с действующими на момент разработки или модернизации Системы настройками.

4.4.2. Разрабатываемые плагины не должны содержать недокументированных возможностей, направленных на скрытый контроль пользователей или администраторов Системы.

4.4.3. Свободно распространяемые и проприетарные программные элементы (библиотеки, скрипты и т.п.), используемые в составе плагина, рекомендуется выбирать с учетом наличия заключения производителя или третьей стороны об отсутствии уязвимостей и недокументированных возможностей.

4.4.4. При функционировании плагинов должны быть запущены только те сервисы/службы/процессы/приложения, которые необходимы для его штатной эксплуатации.

4.5. Требования к аудиту

4.5.1. В ЕАС ОПС и Системах, с которыми взаимодействует данный плагин, должен быть включен механизм протоколирования событий.

4.5.2. В ЕАС ОПС как минимум должны протоколироваться следующие события:

- запуск плагина;
- работа пользователей с данными в плагине, в том числе создание, чтение, изменение или удаление данных, в первую очередь операции, связанные с проведением финансовых транзакций и обработкой ПДн;
- события аутентификации пользователя в плагине, выход (окончание сессии) из плагина, если технически применимо;

- действия привилегированных пользователей по настройке и изменению конфигурации плагина, в том числе изменение настроек плагина, настроек аудита, создание/удаление пользователей/ролей/групп пользователей, изменение привилегий пользователей/ролей/групп пользователей, установка/удаление компонентов плагина;

- доступ к записям журнала протоколирования событий.

4.5.3. В Системе при взаимодействии с плагином как минимум должны протоколироваться следующие события:

- события аутентификации пользователя плагина, выход (окончание сессии) из плагина, если технически применимо;

- работа пользователей с данными в плагине, в том числе создание, чтение, изменение или удаление данных, в первую очередь операции, связанные с проведением финансовых транзакций и обработкой ПДн;

- в случае аутентификации пользователей плагина на стороне Системы
- действия привилегированных пользователей по созданию/ удалению пользователей/ролей/групп пользователей, изменению привилегий пользователей/ролей/групп пользователей, настройке аудита;

- доступ к записям журнала протоколирования событий.

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

4.5.5. По каждому событию должна протоколироваться следующая информация:

- результат операции (успешно/неуспешно);

- идентификатор источника операции (идентификатор пользователя, логин пользователя, имя процесса, а также IP-адрес или идентификатор рабочей станции и т.д.);

- идентификатор объекта, над которым была выполнена операция;

- название и тип выполненной операции (например, аутентификация, чтение, запись, удаление, установление соединения и др.);

- значение параметра до и после операции, если действие предполагает изменение данных или состояния компонентов плагина;

- дата и время выполнения операции, включая указание часового пояса.

4.5.6. Время, указываемое в журналах аудита, должно быть синхронизировано с системным временем домен-контроллера или корпоративного NTP-сервера, если технически реализуемо.

4.5.7. Срок хранения журналов аудита в оперативном доступе в локальном журнале ЕАС ОПС или Системы, с которой взаимодействует плагин, должен составлять не менее трех месяцев.

4.5.8. Должна быть предусмотрена возможность сохранять логины журналов аудита Системы, с которой взаимодействует плагин, во внешние системы.

4.5.9. Журналы аудита плагинов не должны содержать данных конфиденциального характера (например, пароли пользователей).

4.6. Требования к web-приложениям

4.6.1. При взаимодействии плагина с web-интерфейсами или приложениями дополнительно должно быть обеспечено выполнение требований приложения № 1 к Стандарту 1.

4.7. Требования к документации и исходным кодам

4.7.1. Требования к документации и исходным кодам определены соответствующим разделом Стандарта 1.

4.8. Требования к ИСПДн

4.8.1. Требования ИБ к плагину в случае обработки в нем ПДн определены соответствующим разделом Стандарта 1.

4.8.2. При передаче персональных данных по сетям общего пользования должна быть обеспечена защита с использованием средств криптографической защиты информации, имеющих сертификат соответствия ФСБ России.

4.8.3. В качестве альтернативного решения для защиты передачи данных по сетям общего пользования можно применять обезличивание информации в соответствии с приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и методическими рекомендациями к нему.

4.9. Требования к исполнителю работ

4.9.1. Требования к исполнителю работ по созданию или модификации плагина определены соответствующим разделом Стандарта 1.

Описание реализации требований ИБ
Стандарта обеспечения информационной безопасности при разработке
или модернизации плагинов ЕАС ОПС АО «Почта России»
для плагина «название плагина»

Пункт Стандарта	Требования (вопросы)	Реализация (ответ)
Общие требования		
4.1.1	Должна осуществляться проверка/валидация любых входных данных на длину, допустимые символы, кодировку, полноту данных (наличие обязательных параметров). Проверка должна осуществляться до процесса их обработки в плагине и передачи во внешние компоненты	Да, запрашивается ввод логина и пароля
4.1.2	Возможность управления сервисами безопасности, в том числе отключения, подключения, модификации режима аутентификации, авторизации, аудита и т.п., должна быть доступна только администратору плагина	Да, управление сервиса безопасности доступно только роль администратора
Требования к аутентификации и авторизации		
4.2.1	Доступ к функционалу плагина должен предоставляться только после успешного прохождения процесса аутентификации пользователя и последующей его авторизации? Все действия в плагинах должны производиться с использованием учетных записей, наделенных минимально необходимыми привилегиями?	Да, запуск плагина возможен только при успешной аутентификации (логин/пароль) в ЕАС ОПС. Плагин запускается из-под непривилегированной локальной УЗ
4.2.1	Прохождение аутентификации пользователя осуществляется в ЕАС ОПС или в Системе, с которой взаимодействует плагин?	Применяется собственная локальная аутентификация (логин/пароль) в ЕАС ОПС
...	...	...
...	...	...