ОПОИБ

1. курс, 9 группа, ММАД

19 Вариант

Крагель Алина

**Структура документов по безопасности информационных систем (Основные положения стандарта СТБ ISO/IEC 27002-2012). Документ "Процедуры реагирования в случае инцидентов".**

Предназначен для определения порядка реагирования персонала предприятия на возникающие в процессе работы инциденты. Вид документа – инструкция. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Пересматривается и актуализируется по необходимости.

Состав документа.

*Возможные ситуации*

Процедуры должны предусматривать все возможные ситуации, включая:

* сбои в информационных системах
* отказ в обслуживании
* ошибки из-за неполных или неправильных входных данных
* утечку информации

*Оперативный план восстановления системы после инцидента*

В дополнении к оперативному плану восстановления процедуры должны также включать:

* анализ и определение причин инцидента
* планирование и внедрение мер для предотвращения повторения (если необходимо)
* анализ и сохранение сведений об инциденте, которые можно представить в качестве доказательства (улики, свидетельства и т.п.)
* определение порядка взаимодействия между пострадавшими от инцидента и участниками процесса восстановления
* обязательное информирование ответственных лиц

*Сбор информации по инциденту*

По каждому инциденту должно быть собрано максимальное количество информации, которой также необходимо обеспечить необходимый уровень защиты для:

* последующего анализа внутренних проблем
* использования собранных данных для привлечения виновных к дисциплинарной, административной или уголовной ответственности
* использования при ведении переговоров о компенсациях с поставщиками аппаратного и программного обеспечения

*Действия по восстановлению после обнаружения уязвимостей в системе безопасности, исправлению ошибок и ликвидации неисправностей должны быть внимательно и формально запротоколированы.*

Процедура должна гарантировать что:

* только персонал, прошедший процедуры идентификации и аутентификации может получать доступ к “ожившим” системам и данным
* все действия по выходу из нештатной ситуации зафиксированы в виде документа для последующего использования
* обо всех произведенных действиях руководство было проинформировано в установленном порядке
* целостность и работоспособность системы подтверждена в минимальные сроки

**Технология мобильной электронной цифровой подписи. Порядок использования сервера авторизации для идентификации и аутентификации пользователя.**

Мобильная ЭЦП - технология, которая позволяет гражданам использовать мобильный телефон в качестве надежного средства электронной цифровой подписи и для идентификации при получении услуг через Интернет или в устройствах самообслуживания (инфокиосках). В Республике Беларусь технология мобильной ЭЦП создана ЗАО «АВЕСТ» совместно с унитарным предприятием «Велком» (А1) и республиканским унитарным предприятием «Национальный центр электронных услуг». Абоненты А1 и МТС имеют возможность подключить услугу SIMiD для доступа к системе мобильной ЭЦП. Для этого абонент должен обратиться в уполномоченный центр обслуживания клиентов для смены SIM на специализированную SIM с функцией ЭЦП, при этом телефонный номер сохраняется за абонентом. Владелец SIM с подключенной услугой SIMiD может обратиться в любой регистрационный центр (далее - РЦ) республиканского удостоверяющего центра (далее - РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее - ГосСУОК), имеющий подключение к системе мобильной ЭЦП, для генерации ключей ЭЦП и выпуска сертификата открытого ключа. Услуги РЦ РУЦ ГосСУОК могут быть оказаны владельцу SIM непосредственно в уполномоченном центре обслуживания клиентов А1 и МТС.

Задачи

Технология мобильной ЭЦП решает те же задачи, что и другие технологии ЭЦП: возможность пройти аутентификацию с использованием сертификата открытого ключа и возможность выработать ЭЦП. С точки зрения удобства, главным отличием мобильной ЭЦП от других технологий является простота использования: нет необходимости в отдельном средстве ЭЦП (смарт-карте или USB-токене), не требуется установка и настройка программного обеспечения, все функции ЭЦП выполняет специализированная SIM- карта в мобильном телефоне. Технология мобильной ЭЦП может быть использована с любого компьютера, планшета или смартфона. С точки зрения безопасности, главным преимуществом технологии мобильной ЭЦП является обязательность физического использования владельцем SIM своего телефона при любых операциях ЭЦП: он должен вводить известные только ему PIN- коды только на собственном мобильном телефоне. Это делает технологию мобильной ЭЦП более стойкой по сравнению с другими технологиями ЭЦП.

Организационная структура мобильной ЭЦП

Организационную инфраструктуру мобильной ЭЦП образуют:

* *Мобильный оператор*. Мобильный оператор предоставляет услуги связи на основе специализированной SIM, включая услуги передачи специализированных бинарных SMS.
* *Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь*. ГосСУОК (включая регистрационные центры мобильного оператора) осуществляют операции управления ключами на SIM и выпускают сертификаты открытых ключей.
* *Сервер авторизации ГосСУОК*. Сервер авторизации ГосСУОК предоставляет сервис идентификации и аутентификации владельцев SIM с функцией ЭЦП и сервис выработки ЭЦП. Сервер авторизации осуществляет взаимодействие с мобильным оператором для передачи специализированных бинарных SMS на SIM, также взаимодействует с ГосСУОК для получения сертификатов открытых ключей SIM и информации об их статусе.
* *Поставщики электронных услуг*. Поставщикам требуется надежная идентификация и аутентификация своих пользователей, а также возможность выработки ЭЦП пользователем с соблюдением требований Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи».
* *Абоненты мобильного оператора*, использующие SIM-карты с функцией ЭЦП. Абоненты мобильного оператора, в случае получения SIM с функций ЭЦП, могут использовать сервер авторизации для надежной идентификации и аутентификации перед поставщиком электронных услуг, а также для выработки ЭЦП.

*Технология мобильной ЭЦП*

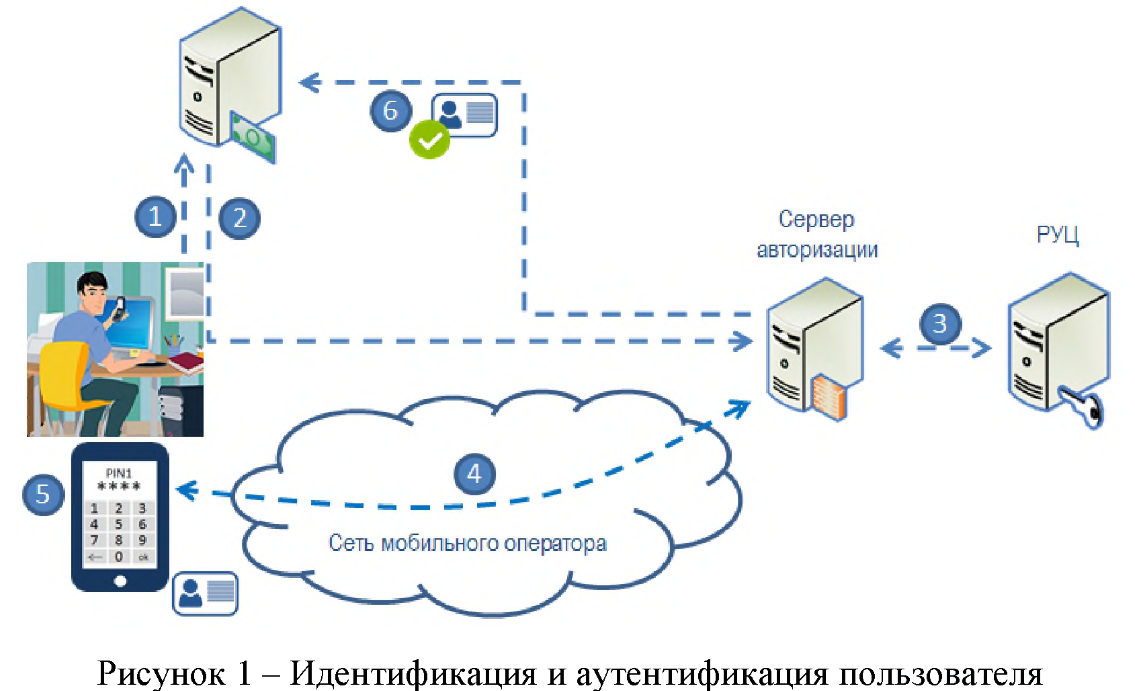
SIM с функцией ЭЦП создана на основе высокопроизводительного защищенного микроконтроллера. SIM соответствует стандартам GSM/3GPP/LTE (2G/3G/4G) в части услуг связи. Дополнительно SIM содержит приложение ЭЦП, которое соответствует спецификации SIM Application Toolkit согласно стандартам GSM/3GPP/LTE (2G/3G/4G). Приложение ЭЦП хранит личный ключ ЭЦП и выполняет криптографические операции с личным ключом: все операции выполняются только внутри SIM, личный ключ не покидает пределов SIM. Для проведения операций входные данные должны быть переданы на SIM в виде служебных («бинарных») SMS согласно 3GPP TS 23.040, результаты обработки возвращаются также в виде «бинарных» SMS. Приложение ЭЦП на SIM реализует сервис идентификации и аутентификации владельца SIM с использованием сертификата открытого ключа согласно СТБ 34.101.19 -2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»

После завершения аутентификации приложение ЭЦП на SIM устанавливает защищенное соединение1 с сервером авторизации с использованием криптографических алгоритмов и протоколов согласно:

* СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»,
* СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»,
* СТБ 34.101.47-2017 «Информационные технологии и безопасность. Алгоритмы генерации псевдослучайных чисел».

Приложение ЭЦП на SIM также реализует сервис выработки ЭЦП электронного документа согласно СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»: приложение ЭЦП вырабатывает ЭЦП для хэш-значения, присланного сервером по защищенному соединению в бинарной SMS, выработанное значение ЭЦП возвращается на сервер также по защищенному соединению. Формат формируемого электронного документа соответствует требованиям СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений». Для подтверждения своего согласия на прохождение идентификации и аутентификации владелец SIM должен ввести на телефоне PIN 1, для подтверждения своего согласия на выработку ЭЦП — ввести PIN2. Длина PIN1 составляет 4 цифры, PIN2 — 5 цифр. После 5 неудачный попыток ввода каждого PIN-кода доступ к сервисам идентификации/аутентификации и выработки ЭЦП блокируется. PIN коды могут быть разблокированы путем ввода PUK-кода. После 3-х неудачный попыток ввода PUK-кода приложение ЭЦП на SIM блокируется. Сервер авторизации предоставляет поставщикам услуг программный интерфейс для идентификации и аутентификации владельцев SIM, для выработки ими электронной цифровой подписи. Программный интерфейс сервера авторизации доступен по протоколу Oauth2 с обеспечением защиты информации по протоколу TLS согласно СТБ 34.101.65-2014 «ИБ. Протокол защиты транспортного уровня (TLS)». В целом, SIM с функцией ЭЦП во взаимодействии с сервером авторизации реализует набор национальных стандартных криптографических алгоритмов в соответствии с Положением о криптографической защите информации Оперативно-¬аналитического центра при Президенте Республики Беларусь (приказ Оперативно- аналитического центра при Президенте Республики Беларусь 30.08.2013 № 62 в редакции приказа 16.01.2015 № 3).

Порядок использования сервера авторизации для идентификации и аутентификации пользователя

****

1. Пользователь, который является владельцем SIM с ЭЦП, обращается на электронный ресурс поставщика за услугой.
2. Поставщик перенаправляет пользователя на сервер авторизации с обращением к сервису идентификации и аутентификации сервера. Пользователь указывает серверу свой телефонный номер.
3. Сервер определяет сертификат, выпущенный на данный телефонный номер, и проверяет его статус.
4. Сервер выполняет протокол аутентификации пользователя путем обмена с SIM бинарными SMS.
5. Для подтверждения согласия на прохождение идентификации и аутентификации на сервере с последующей передачей своих идентификационных данных поставщику услуг владелец SIM вводит на телефоне PIN1.
6. Сервер возвращает поставщику услуг результат аутентификации пользователя и подлинные идентификационные данные пользователя: Ф.И.О., паспортные данные, сертификат открытого ключа ЭЦП и др.