

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ  
(БАНК РОССИИ)

УТВЕРЖДЕН  
ВАМБ.00108-06-ЛУ

**СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
АВТОМАТИЗИРОВАННЫХ СИСТЕМ БАНКА РОССИИ  
«ЯНТАРЬ» ВЕРСИЯ 6**

ДЕЙСТВИЯ ПЕРСОНАЛА В НЕШТАТНЫХ СИТУАЦИЯХ

Инструкция

ВАМБ.00108-06 97 02

2019

## **Аннотация**

Настоящая инструкция определяет согласованный порядок действий абонентов и управляющего персонала при эксплуатации программного комплекса (ПК) ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6» (далее по тексту - СКЗИ «Янтарь») при возникновении нештатных ситуаций.

## **Содержание**

<b>1</b>	<b>ДЕЙСТВИЯ ПЕРСОНАЛА В НЕШТАТНЫХ СИТУАЦИЯХ</b>	<b>4</b>
<b>2</b>	<b>РЕГИСТРАЦИОННЫЕ ЖУРНАЛЫ</b>	<b>7</b>
	<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ</b>	<b>7</b>

# 1 ДЕЙСТВИЯ ПЕРСОНАЛА В НЕШТАТНЫХ СИТУАЦИЯХ

Действия персонала в нештатных ситуациях приведены ниже (Таблица 1).  
Таблица 1 – Действия персонала в нештатных ситуациях

№	Нештатная ситуация	Действия персонала
1	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера	Остановить криптосервер (КС) и все ЭВМ с установленной СКЗИ «Янтарь». Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители и личные идентификаторы ответственному за эксплуатацию СКЗИ «Янтарь» (или лицу его заменяющему). Ответственный за эксплуатацию СКЗИ «Янтарь» (или лицо его заменяющее) организует комиссию по упаковке всех носителей ключевой информации (в том числе и резервных, а также и регистрационных карточек ключей проверки электронной подписи (ЭП) пользователей), предварительно помещённых пользователями в опечатываемый контейнер, который выносится в безопасное помещение или здание до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств. Ответственный за эксплуатацию СКЗИ «Янтарь» (или лицо его заменяющее) оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ «Янтарь», ответственный за эксплуатацию СКЗИ «Янтарь» организует уничтожение всех ключевых носителей, находящихся в контейнере.
2	Компрометация ключа ЭП	Порядок действий при компрометации ключей описан в документе ВАМБ.00108-06 97 01 «СКЗИ «Янтарь» версия 6. Управление ключевой системой. Инструкция».
3	Выход из строя личного носителя ключевой информации	Необходимо оповестить администратора информационной безопасности, сообщить по телефону в подразделение, обеспечивающее управление ключевой системой о факте выхода из строя личного ключевого носителя. Для работы рекомендуется изготовить с оригинала очередную рабочую копию ключа взамен вышедшей из строя.
4	Выход из строя одновременно всех личных носителей ключевой информации	Необходимо оповестить администратора информационной безопасности, сообщить по телефону в подразделение, обеспечивающее управление ключевой системой о выходе из строя всех личных ключевых носителей. Для работы следует провести повторную регистрацию пользователя.
5	Компрометация ключевых документов всех пользователей данной ЭВМ с установленным ПК «Средство КЗИ»	Пользователи, у которых скомпрометированы ключевые документы, останавливают работу ЭВМ с установленным ПК «Средство КЗИ», оповещают администратора безопасности и являются в подразделение, обеспечивающее управление ключевой системой для новой регистрации.

№	Нештатная ситуация	Действия персонала
6	Отказы и сбои в работе аппаратной части КС и ЭВМ с установленным ПК «Средство КЗИ»	При отказах и сбоях в работе аппаратной части КС и ЭВМ с установленным ПК «Средство КЗИ», необходимо остановить работу ЭВМ, перевести работу на резервный КС или ЭВМ (если имеется). По возможности локализовать неисправность, произвести ремонт и переустановку программного обеспечения (ПО) и ключевой системы.
7	Случайные одиночные сбои в работе аппаратной части и системных программных средств	При обработке, хранении и пересылке данных возможно их искажение за счет случайных сбоев оборудования и системного ПО. Эти сбои и искажения с низкой, но ненулевой вероятностью, могут быть не зафиксированы средствами программного и аппаратного контроля и выявлены только косвенно, при криптографическом контроле целостности данных. Организации, разрабатывающей и эксплуатирующей прикладные системы с использованием ПК «Средство КЗИ», рекомендуется разработать инструкции по действию персонала в случаях выявления таких одиночных сбоев. В случае регулярного повторения сбоев и искажения информации рекомендуется провести тестирование оборудования и системного ПО и, при необходимости, провести ремонт или замену оборудования с высоким уровнем случайных сбоев.
8	Отказы и сбои в работе СЗИ от НСД	При отказах и сбоях в работе средств защиты информации (СЗИ) от несанкционированного доступа (НСД) необходимо произвести замену СЗИ от НСД на исправные.
9	Утеря личного ключевого носителя или идентификатора СЗИ от НСД	Утеря личного ключевого носителя или идентификатора СЗИ от НСД равносильна компрометации ключевых документов. В этом случае необходимо руководствоваться документом ВАМБ.00108-06 97 01 «СКЗИ «Янтарь» версия 6. Управление ключевой системой. Инструкция».
10	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в ПО	При отказах и сбоях в работе программных средств вследствие не выявленных ранее ошибок в программном обеспечении (ПО), необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.
11	Отказы в работе ПО вследствие случайного или умышленного его искажения	При отказах в работе ПО вследствие случайного или умышленного его искажения лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы ПО в установленном порядке.
12	Отказы в работе ПО вследствие ошибок оператора	При отказах в работе ПО вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы ПО в установленном порядке.

№	Нештатная ситуация	Действия персонала
13	Сообщения об ошибках, фиксируемых ПК «Автоматизированное рабочее место управления крипто-сервером» (АРМ УКС)	Сообщения об ошибках, фиксируемых АРМ УКС, должны заноситься в журнал. О фактах регистрации сообщений об ошибках администраторы сообщают ответственному за эксплуатацию СКЗИ «Янтарь» или его заместителю.

## **2 РЕГИСТРАЦИОННЫЕ ЖУРНАЛЫ**

Все нештатные ситуации должны отражаться в соответствующих журналах.

Рекомендуемые формы журналов и описание отражаемых в них сведений приведены в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности».

Основные сведения о ведении журналов при эксплуатации СКЗИ «Янтарь» приведены в документе ВАМБ.00108-06 97 01 «СКЗИ «Янтарь» версия 6. Управление ключевой системой. Инструкция».

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

АРМ	Автоматизированное рабочее место
АРМ УКС	АРМ управления криптографическим сервером
КС	Криптографический сервер
НСД	Несанкционированные действия
ПК	Программный комплекс
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СКЗИ	Система криптографической защиты информации
ЭП	Электронная подпись



[illegible]