р
ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА
ПО МОСКОВСКОЙ ОБЛАСТИ
(УФК по Московской области)
ПРИКАЗ
ОМ вере оО г, № 5595
Москва
Об утверждении руководящих документов по эксплуатации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь»

Во исполнение требований Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 №152 и технической и эксплуатационной документации к системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» Управления Федерального казначейства по Московской области приказываю:

1. Возложить на начальника Отдела режима секретности и безопасности информации Управления Федерального казначейства по Московской области функции по хранению первых экземпляров ключевых документов к системе криптографической защиты информации автоматизированных систем Банка России «Янтарь».

2. Утвердить:

2.1. Инструкцию администратора безопасности информации системы 046001

криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области согласно приложению № 1 к настоящему приказу.

2.2. Инструкцию администратора объекта информационной инфраструктуры системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области согласно приложению № 2 к настоящему приказу.

2.3. Инструкцию операторов ключевой системы и администраторов криптосервера системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области согласно приложению №3 к настоящему приказу.

2.4. Порядок обращения с ключевыми документами и ключевыми носителями системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» согласно приложению № 4 к настоящему приказу.

2.5. Инструкцию по эксплуатации (применению) комплекса средств защиты информации |: системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» согласно приложению № 5 к настоящему приказу.

2.6. Общие организационные меры по обеспечению безопасности информации при эксплуатации системы — криптографической защиты — информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области согласно приложению №6 к настоящему приказу.

2.7. Инструкцию по организации назначения (Удаления) учетных записей пользователям и парольной защиты в системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» Управления Федерального казначейства по Московской области согласно приложению № 7 к настоящему приказу.

2.8. Перечень мероприятий по проведению контроля в системе

3
’ криптографической защиты информации автоматизированных систем Банка России «Янтарь» согласно приложению № 8 к настоящему приказу.

3. Признать утратившим силу Приказ Управления Федерального казначейства по Московской области от 31.12.2020 № 1273 «Об утверждении руководящих документов по эксплуатации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь».

4. Контроль за исполнением приказа оставляю за собой.

Руководитель | В.А. Мартьянова

Приложение № 1
УТВЕРЖДЕНА
приказом УФК
по Московской области
от «04 Мебля 2021г.№ 295.
Инструкция
администратора безопасности информации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области
Г. Общие положения

1.1. Настоящая Инструкция разработана на основании требований ВАМБ.О0108-06 93 01 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6. Руководство администратора информационной безопасности» и регламентирует основные права, обязанности и ответственность администратора безопасности информации, системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») в Управлении Федерального казначейства по Московской области (далее — Управление).

1.2. Администрирование безопасности СКЗИ «Янтарь» осуществляется сотрудником, допущенным к работе со средствами криптографической защиты информации и назначенным администратором безопасности СКЗИ «Янтарь» приказом Управления.

1.3. Администратор безопасности назначается из числа сотрудников отдела режима секретности и безопасности информации (далее — отдел РСиБИ) и является лицом, выполняющим функции по обеспечению и контролю безопасности информации, обрабатываемой, передаваемой и хранимой в СКЗИ «Янтарь».

1.4. В своей деятельности администратор безопасности руководствуется требованиями настоящей Инструкции, а также действующих федеральных законов, общегосударственных, ведомственных и внутренних нормативных документов по

вопросам защиты информации и контролирует их выполнение администраторами криптосервера, администраторами объекта информационной инфраструктуры, операторами автоматизированного рабочего места управления криптосервером и владельцев ключей Управления СКЗИ «Янтарь».
П. Права и обязанности администратора безопасности информации

2.1. Администратор безопасности информации обязан:

2.1.1. Знать перечень задач по обработке информации, содержащей сведения, конфиденциального характера, не составляющую государственную тайну (далее - конфиденциальная информация) решаемых в СКЗИ «Янтарь», согласно эксплуатационной и технической документации к ней.

2.1.2. Знать состав СКЗИ «Янтарь», не допускать случаев включения в ее состав блоков и устройств без согласования с начальником Отдела РСиБИ и начальником Отдела информационных систем (далее — ИС).

2.1.3. Пресекать использование нелицензионного программного обеспечения.

2.1.4. Совместно с администраторами объекта информационной инфраструктуры определить состав регистрируемых событий и списка лиц, имеющих допуск к журналам аудита.

2.1.5. Организовывать учет, хранение, прием и выдачу персональных идентификаторов, осуществлять контроль за правильностью их использования.

2.1.6. Осуществлять периодический контроль за порядком учета, создания, хранения и использования основных и резервных копий ключевых документов.

2.1.7. Контролировать выполнение требований действующих нормативных документов но вопросам защиты информации при её обработке в СКЗИ «Янтарь».

2.1.8. Осуществлять методическое руководство работой администраторов и операторов СКЗИ «Янтарь» в вопросах обеспечения информационной безопасности. Проводить периодический инструктаж администраторов и операторов СКЗИ «Янтарь» по правилам работы с используемыми средствами и системами зашиты информации.

2.1.9. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в СКЗИ «Янтарь» в пределах возложенных функций. В случае отказа этих средств и систем принимать меры по их восстановлению.

2.1.10. Проводить периодический контроль средств вычислительной техники, входящих в состав СКЗИ «Янтарь» на предмет несанкционированного изменения установленного программного обеспечения, а также их состава, конфигурации и размещения.

2.1.11. Периодически контролировать целостность печатей (пломб, наклеек) на серверах, рабочих станциях и коммуникационном оборудовании, входящем в состав СКЗИ «Янтарь».

2.1.12. Осуществлять оперативный контроль за работой администраторов и операторов СКЗИ «Янтарь», анализировать содержимое журналов аудита операционных систем рабочих станций и серверов СКЗИ «Янтарь», прикладного программного обеспечения, функционирующего в СКЗИ «Янтарь».

2.1.13. Своевременно информировать начальника Отдела РСиБИ о несанкционированных действиях администраторов и операторов.

2.2. Администратору безопасности информации запрещается:

2.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей.

2.2.2. Использовать ставшие доступными в ходе исполнения обязанностей идентификационные и аутентификационные данные администраторов и операторов СКЗИ «Янтарь» (имя, пароль и т.п.) для маскирования своих действий.

2.2.3. Самостоятельно (без согласования с начальником Отдела РСиБИ и Отдела ИС) вносить изменения в настройки и состав основных технических средств.

2.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы СКЗИ «Янтарь», предоставлять такую возможность другим.

2.2.5. Выключать средства защиты информации от несанкционированного доступа без санкции начальника отдела РСИБИ.

2.2.6. Передавать третьим лицам тем или иным способом сетевые адреса,

имена, пароли, информацию о привилегиях администраторов и операторов СКЗИ «Янтарь», конфигурационные настройки рабочих станций, серверов, периферийного и коммуникационного оборудования СКЗИ «Янтарь».
2.2.7. Нарушать правила эксплуатации оборудования СКЗИ «Янтарь».
2.2.8. Корректировать, удалять, подменять журналы аудита объекта СКЗИ «Янтарь».
2.3. Администратор безопасности информации имеет право:
2.3.1. Получать доступ к программным и аппаратным средствам СКЗИ «Янтарь», средствам их защиты, а также просматривать права доступа пользователей к программным и анпаратным средствам СКЗИ «Янтарь».
2.3.2. Требовать от администраторов и операторов СКЗИ «Янтарь» выполнения инструкций по обеспечению безопасности и защите информации в СКЗИ «Янтарь».
2.3.3. Инициировать и участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности.
2.3.4. Осуществлять оперативное вмешательство в работу пользователя СКЗИ «Янтарь», если его действия создают угрозу безопасности информации, с последующим докладом начальнику Отдела РСиБИ.
2.3.5. Производить анализ защищенности СКЗИ «Янтарь» путем применения специальных программных и технических средств.
2.3.6. Вносить свои предложения по совершенствованию мер защиты информации в СКЗИ «Янтарь».
Ш. Ответственность администратора безопасности информации
3.2. Администратор безопасности информации несет ответственность за:
3.2.1. Реализацию принятой в Управлении политики информационной безопасности.
3.2.2. Качество проводимых им работ по обеспечению защиты СКЗИ «Янтарь» в соответствии с функциональными обязанностями.
|
ООО

| Приложение № 2
УТВЕРЖДЕНА
приказом УФК
по Московской области
от« (7% Себе ф 2021 г. № 9595)
Инструкция
администраторов объекта информационной инфраструктуры системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области
1. Общие положения

1.1. Настоящая Инструкция разработана на основании требований ВАМБ.О0108-06 95 01 «Система криптографической защиты информации автоматизированных систем банка России «Янтарь» версия 6. Автоматизированное рабочее место управления криптографическим сервером. Автоматизированное рабочее место формирования отчетов. Руководство по установке и настройке» и регламентирует основные обязанности и ответственность администратора объекта информационной инфраструктуры (далее — Администратор ОИИ), системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») в Управлении Федерального казначейства по Московской области (далее — Управление).

1.2. Обработка сведений конфиденциального характера в СКЗИ «Янтарь» осуществляется оператором, допущенным к работе с СКЗИ «Янтарь» приказом Управления.

1.3. Администраторы ОИИ в своей работе руководствуются, действующими нормативными и организационно-распорядительными документами по вопросам информационной безопасности, должностными и технологическими инструкциями.

1.4. К работе с криптосредствами допускаются работники Управления, прошедшие обучение (инструктаж) по вопросам защиты информации с применением криптосредств.

1.5. Требования настоящей Инструкции обязательны для исполнения всеми Администраторами ОИИ, допущенными к работе к СКЗИ «Янтарь», и доводятся до них под роспись.

П. Обязанности администраторов ОИИ

2.1. При выполнении работ в СКЗИ «Янтарь» Администраторы ОЙИИ обязаны:

2.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами, правила работы и порядок регистрации, доступа к информационным ресурсам, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.1.2. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним, и других мерах защиты информации.

2.1.3. Знать и строго выполнять правила работы со средствами защиты информации (далее — СЗИ), средствами криптографической защиты информации (далее — СКЗИ), установленными в СКЗИ «Янтарь».

2.1.4. Выполнять требования нормативных документов по организации парольной защиты в Управлении, осуществлять регистрацию на автоматизированных рабочих местах СКЗИ «Янтарь» только под своими идентификационными (учетными) данными.

2.1.5. Передавать для хранения установленным порядком индивидуальное устройство идентификации Тоиср Метогу, персональные ключевые носители и другие реквизиты разграничения доступа в пенале, опечатанном личной печатью, только начальнику структурного подразделения.

2.1.6. Надежно хранить и никому не передавать личную печать.

2.1.7. Выполнять требования нормативных документов по организации антивирусной защиты в Управлении.

2.1.8. Немедленно вызывать администратора безопасности СКЗИ «Янтарь» и ставить в известность начальника структурного подразделения в случае утери

персонального ключевого носителя, индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушения целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах СКЗИ «Янтарь» или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее — НСД) к защищенным средствам вычислительной техники СКЗИ «Янтарь»; несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств вычислительной техники; некорректного функционирования СЗИ, СКЗИ, установленных на средствах вычислительной техники.

2.1.9. Ставить в известность администратора безопасности СКЗИ «Янтарь» при необходимости внесения изменения в состав аппаратных и программных средств СКЗИ «Янтарь» или о проведении работ по внесению таких изменений.

2.1.10. Работать в СКЗИ «Янтарь» только в разрешенный период времени.

2.1.11. Немедленно выполнять предписания администратора безопасности СКЗИ «Янтарь», предоставлять средства вычислительной техники администратору безопасности СКЗИ «Янтарь» для контроля.

2.1.12. Ставить в известность администраторов безопасности СКЗИ «Янтарь» в случае появления сведений или подозрений о фактах НСД к информации, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию средств вычислительной техники, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (клавиатура, манипулятор и т.п.).

2.1.13. Осуществлять уничтожение информации, содержащей сведения ограниченного доступа, с машинных носителей информации и из оперативной памяти, в установленном Управлении порядке.

2.1.14. Сдавать в Отдел режима секретности и безопасности информации криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.1.15. Сообщать начальнику Отдела информационных систем и начальнику Отдела режима секретности и безопасности информации обо всех проблемах, связанных с эксплуатацией СКЗИ «Янтарь».

2.1.16. Контролировать целостность печатей (пломб, наклеек) на средствах вычислительной техники и коммуникационном оборудовании, входящем в состав СКЗИ «Янтарь».

2.2. Администраторам ОИИ запрещается:

2.2.1. Использовать компоненты программного и аппаратного обеспечения СКЗИ «Янтарь» в неслужебных целях.

2.2.2. Самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств СКЗИ «Янтарь» (в том числе серверов), или устанавливать дополнительно любые программные и аппаратные средства.

2.2.3. Осуществлять обработку информации, содержащей сведения ограниченного доступа, в присутствии посторонних (не допущенных к данной информации) лиц.

2.2.4. Использовать неучтенные машинные носители информации.

2.2.5. Оставлять включенными без присмотра средства вычислительной техники, не активизировав временную блокировку экрана (средствами защиты от НСД или операционных систем).

2.2.6. Передавать кому-либо свои персональные ключевые носители в нарушение установленного порядка, делать неучтенные копии, вносить какие-либо изменения в структуру и файлы ключевых носителей.

2.2.7. Оставлять без личного присмотра персональные ключевые носители, персональное устройство идентификации, съёмные машинные носители информации и документы, содержащие защищаемую информацию (в т.ч. сведения ограниченного доступа).

2.2.8. Допускать записи на ключевой носитель посторонней информации.

2.2.9. Умышленно использовать недекларированные возможности, ошибки в программном обеспечении или в настройках СКЗИ «Янтарь» (включая средства

защиты информации), которые могут привести к нарушению или к созданию предпосылок для нарушения функционирования СКЗИ «Янтарь» и являться угрозой для безопасности информации в СКЗИ «Янтарь». При обнаружении такого рода недекларированных возможностей и ошибок, Администратор ОЙИ обязан ставить в известность об этом администратора безопасности СКЗИ «Янтарь» (ответственного за безопасность информации) и начальника Отдела режима секретности и безопасности информации.

2.2.10. Осуществлять попытки НСД к ресурсам СКЗИ «Янтарь».

2.2.11. Разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера.

Ш. Ответственность администраторов ОЙИ

3.1. Администраторы ОИИ несут персональную ответственность за нарушение технологического процесса обработки информации, а также сохранность средств вычислительной техники, периферийного оборудования, используемого им в работе, машинных носителей информации, персональных идентификаторов, ключевых носителей и целостность установленного в СКЗИ «Янтарь» программного обеспечения.

3.2. Ответственность за нарушение функционирования СКЗИ «Янтарь», уничтожение, блокирование, копирование, фальсификацию информации несет Администратор ОИИ, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебной проверки.

3.3. Администраторы ОИИ, виновные в нарушении требований настоящей Инструкции и других документов по защите информации в СКЗИ «Янтарь», несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации, а также организационно-распорядительными документами Управления.

Приложение № 3

УТВЕРЖДЕНА

приказом УФК

по Московской области
от« (4 (6426682021 г. № 59,
Инструкция
операторов ключевой системы и администраторов криптосервера системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области
1. Общие положения

1.1. Настоящая Инструкция разработана на основании требований ВАМБ.о0108-06 95 01 «Система криптографической защиты информации автоматизированных систем банка России «Янтарь» версия 6. Автоматизированное рабочее место управления криптографическим сервером. Автоматизированное рабочее место формирования отчетов. Руководство администратора» и регламентирует основные обязанности и ответственность операторов ключевой системы и администраторов криптосервера (далее — Пользователи КС) системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») в Управлении Федерального казначейства по Московской области (далее — Управление).

1.2. Обработка сведений конфиденциального характера в СКЗИ «Янтарь» осуществляется оператором, допущенным к работе с СКЗИ «Янтарь» приказом Управления.

1.3. Пользователи КС в своей работе руководствуются действующими нормативными и организационно-распорядительными документами по вопросам информационной безопасности, должностными и технологическими инструкциями.

1.4. К работе с криптосредствами допускаются работники Управления прошедшие обучение (инструктаж) по вопросам защиты информации с применением криптосредств.

1.5. Требования настоящей Инструкции обязательны для исполнения всеми Пользователями КС, допущенными к работе к СКЗИ «Янтарь», и доводятся до них под роспись.

П. Обязанности пользователей КС

2.1. При выполнении работ в СКЗИ «Янтарь» Пользователи КС обязаны:

2.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами, правила работы и порядок регистрации, доступа к информационным ресурсам, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.1.2. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты информации.

2.1.3. Знать и строго выполнять правила работы со средствами защиты информации (далее — СЗИ), средствами криптографической защиты информации (далее — СКЗИ), установленными в СКЗИ «Янтарь».

2.1.4. Выполнять требования нормативных документов по организации парольной защиты в Управлении, осуществлять регистрацию на автоматизированных рабочих местах СКЗИ «Янтарь» только под своими идентификационными (учетными) данными.

2.1.5. Передавать для хранения установленным порядком индивидуальное устройство идентификации Тоись Метогу, персональные ключевые носители и другие реквизиты разграничения доступа в пенале, опечатанном личной печатью, только начальнику структурного подразделения.

2.1.6. Надежно хранить и никому не передавать личную печать.

2.1.7. Выполнять требования нормативных документов по организации антивирусной защиты в Управлении.

2.1.8. Немедленно вызывать администратора безопасности СКЗИ «Янтарь» и ставить в известность начальника структурного подразделения в случае утери персонального ключевого носителя, индивидуального устройства идентификации

или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушения целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах СКЗИ «Янтарь» или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее — НСД) к защищенным средствам вычислительной техники СКЗИ «Янтарь»; несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств вычислительной техники; некорректного функционирования СЗИ, СКЗИ, установленных на средствах вычислительной техники.

2.1.9. Ставить в известность администратора безопасности СКЗИ «Янтарь» при необходимости внесения изменения в состав аппаратных и программных средств СКЗИ «Янтарь» или о проведении работ по внесению таких изменений.

2.1.10. Работать в СКЗИ «Янтарь» только в разрешенный период времени.

2.1.11. Немедленно выполнять предписания администратора безопасности СКЗИ «Янтарь», предоставлять средства вычислительной техники администратору безопасности СКЗИ «Янтарь» для контроля.

2.1.12. Ставить в известность администраторов СКЗИ «Янтарь» в случае появления сведений или подозрений о фактах НСД к информации, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию средств вычислительной техники, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (клавиатура, манипулятор и т.п.).

2.1.13. Осуществлять уничтожение информации, содержащей сведения ограниченного доступа, с машинных носителей информации и из оперативной памяти криптосредств, в установленном Управлении порядке.

2.1.14. Сдавать в Отдел режима секретности и безопасности информации криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.1.15. Немедленно прекратить обработку данных с использованием

скомпрометированных ключевых документов.

2.1.16. Сообщать начальнику Отдела режима секретности и безопасности информации обо всех проблемах, связанных с эксплуатацией СКЗИ «Янтарь».

2.1.17. Контролировать целостность печатей (пломб, наклеек) на средствах вычислительной техники и коммуникационном оборудовании, входящем в состав СКЗИ «Янтарь».

2.2. Пользователям КС запрещается:

2.2.1. Использовать компоненты программного и аппаратного обеспечения СКЗИ «Янтарь» в неслужебных целях.

2.2.2. Самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств СКЗИ «Янтарь» (в том числе серверов), или устанавливать дополнительно любые программные и апнаратные средства.

2.2.3. Осуществлять обработку информации, содержащей сведения ограниченного доступа, в присутствии посторонних (не допущенных к данной информации) лиц.

2.2.4. Использовать неучтенные машинные носители информации.

2.2.5. Оставлять включенными без присмотра средства вычислительной техники, не активизировав временную блокировку экрана (средствами защиты от НСД или операционных систем).

2.2.6. Передавать кому-либо свои персональные ключевые носители в нарушение установленного порядка, делать неучтенные копии, вносить какие-либо изменения в структуру и файлы ключевых носителей.

2.2.7. Оставлять без личного присмотра персональные ключевые носители, персональное устройство идентификации, съёмные машинные носители информации и документы, содержащие защищаемую информацию (в т.ч. сведения ограниченного доступа).

2.2.8. Допускать записи на ключевой носитель посторонней информации.

2.2.9. Умышленно использовать недекларированные возможности, ошибки в программном обеспечении или в настройках СКЗИ «Янтарь» (включая средства

защиты информации), которые могут привести к нарушению или к созданию предпосылок для нарушения функционирования СКЗИ «Янтарь» и являться угрозой для безопасности информации в СКЗИ «Янтарь». При обнаружении такого рода недекларированных возможностей и ошибок, Пользователь КС обязан ставить в известность об этом администратора безопасности СКЗИ «Янтарь» (ответственного за безопасность информации) и начальника Отдела режима секретности и безопасности информации.

2.2.10. Осуществлять попытки НСД к ресурсам СКЗИ «Янтарь».

2.2.11. Разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера.

Ш. Ответственность пользователей КС

3.1. Пользователи КС несут персональную ответственность за нарушение технологического процесса обработки информации, а также сохранность средств вычислительной техники, периферийного оборудования, используемого им в работе, машинных носителей информации, персональных идентификаторов, ‘ключевых носителей и целостность установленного в СКЗИ «Янтарь» программного обеспечения.

3.2. Ответственность за нарушение функционирования СКЗИ «Янтарь», уничтожение, блокирование, копирование, фальсификацию информации несет Пользователь КС, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебной проверки.

3.3. Пользователи КС, виновные в нарушении требований настоящей Инструкции и других документов по защите информации в СКЗИ «Янтарь», несут Уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации, а также организационно-распорядительными документами Управления.

Приложение № 4
УТВЕРЖДЕН
приказом УФК
по Московской области
от« 0% ео в 2021г.№ 59,

Порядок
обращения с ключевыми документами и ключевыми носителями системы = криптографической защиты информации автоматизированных систем Банка России «Янтарь»

1. Общие положения

1.1. Настоящий порядок определяет требования к организации и обеспечению безопасности хранения, использования и уничтожения ключевых документов системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») Управления Федерального казначейства по Московской области (далее - Управление).

1.2. Ключевые документы относятся к материальным носителям, содержащим ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов кринтографического преобразования.

1.3. Сотрудник органа криптографической защиты информации (далее — ОКЗИ) ставит на учет и добавляет в имеющиеся лицевые счета пользователей, числящиеся за ним ключевые документы СКЗИ «Янтарь», согласно Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и

| информации при Президенте РФ от 13 июня 2001 г. № 152 (далее — Инструкция 152).

информации, или стиранием содержимого ключевого носителя без повреждения ключевого носителя многократного использования.

3.3. Содержимое ключевых носителей стирают по технологии, принятой для соответствующих ключевых носителей многократного использования в соответствии с эксплуатационной и технической документацией к СКЗИ «Янтарь», а также указаниями отдела режима секретности и безопасности информации Управления.

3.4. Владельцам ключевых документов СКЗИ «Янтарь» разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы.

3.5. Уничтожение по акту производит комиссия в составе не менее двух человек из числа работников отдела режима секретности и безопасности информации Управления. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

|
|
|

Приложение № 5

УТВЕРЖДЕНА

приказом УФК

по Московской области
от« 0.4 (ефвее 2021 г. № 59,
Инструкция
по эксплуатации (применению) комплекса средств защиты информации в системе криптографической защиты информации автоматизированных систем

Банка России «Янтарь»
Т. Общие положения

1.1. Настоящая Инструкция разработана с учетом Положения о системе сертификации средств защиты информации, утвержденного приказом Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55, руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по ‘защите информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992, эксплуатационной и технической документацией на СЗИ, и определяет порядок эксплуатации средств защиты информации (далее — СЗИ), используемых В системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») Управления Федерального казначейства по Московской области (далее — Управление).

1.2. В СКЗИ «Янтарь» применяются сертифицированные Федеральной службой безопасности России СЗИ не ниже 3 класса защиты, внесенные в государственный реестр сертифицированных СЗИ № РОСС ВЦ.0001.01БИ00.

1.3. К СЗИ относятся: технические, программно-аппаратные и программные средства защиты информации, включая средства в которых они реализованы; защищенные средства обработки информации.

1.4. На все СЗИ должны быть в наличии заполненные формуляры

(паспорта), знаки соответствия, заверенные копии сертификатов соответствия. В случае окончания срока действия сертификата соответствия, производителем СЗИ должна осуществляться его техническая поддержка.

1.-. Для каждой версии программно-аппаратных и программных СЗИ должны быть в наличии две копии дистрибутива для восстановления работоспособности системы защиты информации.

1.6. Регулировочные элементы средств активной защиты должны иметь защитные стикеры для обнаружения несанкционированного доступа к ним и электронным компонентам счетчика учета времени наработки, указанные в актах установки СЗИ.

1.7. Управление СЗИ в СКЗИ «Янтарь» осуществляется администратором безопасности в соответствии с эксплуатационной и технической документацией на СЗИ.

1.8. Операторы, администраторы криптосервера, администраторы объекта информационной инфраструктуры, администраторы безопасности обязаны контролировать работоспособность СЗИ перед началом обработки конфиденциальной информации, а также в процессе ее обработки.

1.9. Операторам, администраторам криптосервера, администраторам объекта информационной инфраструктуры, администраторам безопасности запрещено:

обрабатывать информацию в СКЗИ «Янтарь» в случае внештатного функционирования или неисправности СЗИ;

изменять размещение, состав и комплектность СЗИ;

изменять параметры настройки СЗИ, установленные администратором безопасности:

производить вскрытие корпусов узлов и блоков СЗИ;

производить замену отдельных блоков СЗИ;

удалять специальные защитные знаки и гарантийные пломбы.

При выявлении различных неисправностей, ошибок, сбоев в работе СЗИ необходимо прекратить обработку информации ограниченного доступа и сообщить администратору безопасности.

П. Эксплуатация установленного в СКЗИ «Янтарь» средства защиты информации |

2.1. В СКЗИ «Янтарь» установлен и эксплуатируется программно-аппаратный комплекс «Соболь» (далее —- ПАК Соболь).

2.2. Загрузка компьютера и вход пользователя в систему осуществляется с использованием личного идентификатора.

Для загрузки компьютера и входа в систему:

Включите питание компьютера.

На экране появится запрос персонального идентификатора:

Програмыно-аппаратный комплекс "Соболь". Версия 3.0 А
| 1) До окончания входа в систему: 1 мин. 20 сек.

Пояснение.

На рисунке выносками обозначены элементы: 1 — строка сообщений.

Обратите внимание на следующие особенности процедуры входа:

При включенном режиме автоматического входа в строке сообщений будет отсчитываться время в секундах, оставшееся до автоматического входа в ПАК Соболь, после которого начнется загрузка операционной системы;

При включенном режиме ограничения времени, в строке сообщений будет отсчитываться время в минутах и секундах, оставшееся до предъявления идентификатора и ввода пароля. Если вы не успели за отведенное время выполнить

эти действия, на экране появится сообщение «Время сеанса входа в систему истекло». Чтобы повторить попытку входа, нажмите клавишу <Ещег>, а затем — любую клавишу.

Предъявите свой персональный идентификатор.

Если в идентификаторе нет пароля, на экране появится диалог для его ввода:

ИИ

Введите пароль для входа в ПАК Соболь.

Примечание.

На экране каждый символ пароля отображается как «*» (звездочка). Помните, что при вводе пароля различаются строчные и заглавные буквы. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <BacKзрасе> или <Реае> и заново повторите ввод символов.

Нажмите клавишу <Ещег>.

Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение: "Неверный персональный идентификатор или пароль".

Нажмите любую клавишу и снова предъявите идентификатор. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.

Требования к паролям изложены в действующей Инструкции парольной защиты автоматизированной системы, с которой должны ознакомиться все пользователи.

Внимание!

Учитывайте, что число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение в текущем сеансе входа, то при следующей попытке входа в строке сообщений появится сообщение

«Ваш вход в систему запрещен: Вы превысили предел неудачных попыток входа»,

после чего компьютер будет заблокирован. В этом случае обратитесь за помощью к администратору.

После успешного предъявления идентификатора (и ввода правильного пароля, если это необходимо) выполняется тестирование датчика случайных чисел. При обнаружении ошибок в строке сообщений появится сообщение об этом. Если после перезагрузки компьютера тестирование датчика случайных чисел вновь завершилось с ошибкой, обратитесь за помощью к администратору.

Перед загрузкой операционной системы проводится контроль целостности файлов.

Если проверка завершена успешно, начнется загрузка операционной системы. При обнаружении ошибок на экране появятся сообщения об ошибках.

Если в строке сообщений появилось сообщение: «Компьютер заблокирован», - выключите компьютер и обратитесь за помощью к администратору.

При входе в систему пользователь должен указать учетные данные, необходимые для его идентификации. После ввода учетных данных система аутентифицирует пользователя, и при успешном завершении аутентификации предоставляется возможность работы пользователя в системе.

Внимание!

Во время загрузки компьютера до появления экрана приветствия (приглашение на вход в систему) не рекомендуется нажимать какие-— либо клавиши на клавиатуре. Некоторые клавиши могут активировать специальные режимы загрузки, требующие административные полномочия для работы. Чтобы избежать возникновения проблемных ситуаций, выполняйте действия в строгом соответствии с представленным описанием.

Приложение № 6
УТВЕРЖДЕНЫ
| приказом УФК
по Московской области
от «(4 Шиа 2021г. № 29,

Общие организационные меры по обеспечению безопасности информации при эксплуатации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области

При эксплуатации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») установить следующие общие организационные меры:

1. Право доступа к рабочим местам с СКЗИ «Янтарь» предоставлять только лицам, ознакомленным с правилами использования и изучившим эксплуатационную документацию СКЗИ «Янтарь».

2. Запретить использование СКЗИ «Янтарь» для защиты сведений, составляющих государственную тайну.

3. Запретить осуществление несанкционированного администратором информационной безопасности копирования ключевых носителей.

4. Запретить разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.

5. Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ «Янтарь», либо использовать ключевые носители на посторонних средствах вычислительной техники (далее — СВТ).

6. Запретить запись на ключевые носители посторонней информации.

7. На технических средствах, оснащенных СКЗИ «Янтарь», должно использоваться только лицензионное программное обеспечение (далее — ПО) фирм-

производителей.

8. Не устанавливать средства разработки ПО и отладчиков на технических средствах, оснащенных СКЗИ «Янтарь». Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором информационной безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ «Янтарь». Необходимо исключить попадание в СКЗИ «Янтарь» программ, позволяющих, пользуясь ошибками операционной системы (далее - ОС), получать привилегии администратора.

9. Принять меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ «Янтарь», по роду своей деятельности, не являющихся персоналом, допущенным к работе в указанных помещениях.

10. Запретить оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «Янтарь», после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

11. Администратором безопасности должно быть проведено опечатывание системного блока с установленным ПО СКЗИ «Янтарь», исключающее возможность несанкционированного изменения аппаратной части.

12. Оборудование, на которое устанавливается СКЗИ «Янтарь», не должно создавать угрозу безопасности ОС. Недопустимо использовать нестандартные аппаратные средства, имеющие возможность влиять на нормальный ход работы компьютера или ОС.

13. При использовании СКЗИ «Янтарь» на СВТ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых ОС, к ПО, в окружении которого функционирует СКЗИ «Янтарь», и к компонентам СКЗИ «Янтарь» со стороны указанных сетей.

14. В BTO$ СВТ задаются установки, исключающие возможность загрузки ОС,

отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CO-K. и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются СВТ с B!O$, исключающим возможность отключения сетевой загрузки ОС.

15. Средствами ВОЗ должна быть исключена возможность отключения пользователями ТЗА и РСГустройств при использовании средств защиты информации (далее - СЗИ) от НСД, устанавливаемых в [$ A и PC1-разъем.

16. Вход в ВОЗ СВТ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора. Пароль для входа в B1O5 должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.

17. Запретить работу на СВТ, если во время её начальной загрузки не проходят встроенные тесты BTO$.

18. При загрузке ОС должен быть реализован контроль целостности НО, входящего в состав СКЗИ «Янтарь», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ «Янтарь».

19. Физическое затирание содержимого удаляемых файлов СКЗИ «Янтарь» (в том числе, затирание ключевой информации) производить только с помощью конфигурационной программы, входящей в состав Средства СКАД «Сигнатура 6». Описание работы с конфигурационной программой приведено в ВАМБ.00104-06 31 01 «СКАД «Сигнатура 6». «Сигнатура-клиент» версия 6. Средство СКАД «Сигнатура» версия 6. Описание применения».

Приложение № 7
УТВЕРЖДЕНА
приказом УФК
по Московской области
от «04» ее 2021г.№ 29,
Инструкция
по организации назначения (удаления) учетных записей пользователям и парольной защиты в системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» Управления Федерального казначейства по Московской области
Г. Общие положения

1.1. Настоящая Инструкция регламентирует порядок управления учетными записями и парольной защитой в системе криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») Управления Федерального казначейства по Московской области (далее — Управление).

1.2. Настоящая инструкция разработана в соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992, Национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и в целях защиты информации от несанкционированного доступа в информационных (автоматизированных) системах (далее — АС) в зависимости от их класса защищенности и угроз безопасности информации должна осуществляться однозначная идентификация (определение личности) и аутентификация (подтверждение личности) внутренних пользователей СКЗИ «Янтарь» и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от

имени системных учетных записей.

1.3. К внутренним пользователям (далее — пользователь) СКЗИ «Янтарь» относятся:

должностные лица (операторы, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств СКЗИ «Янтарь» в соответствии с должностными регламентами (инструкциями);

лица, привлекаемые на договорной основе для обеспечения функционирования СКЗИ «Янтарь» (ремонт, гарантийное обслуживание, регламентные и иные работы).

1.4. Идентификация пользователя осуществляется по его уникальному идентификатору — учетной записи.

1.-. Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, иных средств.

1.6. Управление — средствами идентификации и аутентификации пользователей осуществляется администратором объекта информационной инфраструктуры (далее — администратор ОИИ) и администратором безопасности, назначаемыми приказом Управления.

П. — Порядок управления учетными записями

2.1. В СКЗИ «Янтарь» используются следующие типы учетных записей: пользователь, гость. В случае производственной необходимости пользователям, могут быть сопоставлены несколько учетных записей. Использование несколькими пользователями одной и той же учетной записи (группового имени) запрещено.

2.2. Порядок заведения учетной записи.

2.2.1. Заведение учетной записи оператора или администратора криптосервера (далее — администратор КС) и предоставление (изменение) ему прав доступа к ресурсам СКЗИ «Янтарь» производится на основании приказа Управления и заявки на допуск к информационным ресурсам АРМ УКС Управления (далее — Заявка)

согласно приложению к настоящей инструкции. На основании Заявки администратор ОИИ СКЗИ «Янтарь» присваивает и сообщает сотруднику Управления его учетную запись для работы в СКЗИ «Янтарь».

2.2.2. Администратор безопасности СКЗИ «Янтарь» проверяет доступные права учетной записи оператора или администратора ОИЙИ согласно технической и эксплуатационной документации к СКЗИ «Янтарь».

2.2.3. Использование обезличенных учетных записей в СКЗИ «Янтарь» не допускается.

2.2.4. Оповещение администратора ОМИ СКЗИ «Янтарь» об изменении сведений об операторах или администраторах КС, их ролях, обязанностях, полномочиях и ограничениях осуществляется начальником соответствующего отдела Управления в виде служебной записки (в случае отстранения от исполняемых функций в СКЗИ «Янтарь» или увольнения начальник соответствующего отдела Управления незамедлительно сообщает в устной форме с последующим представлением приказа об отстранении от исполняемых функций в СКЗИ «Янтарь» или увольнении).

2.2.5. Сотруднику Управления запрещается работа в СКЗИ «Янтарь» под чужой учетной записью. За все действия, произведенные под чужой учетной записью, несет ответственность сотрудник Управления, под чьей учетной записью эти действия производились.

2.3. Активация учетной записи.

2.3.1. После ознакомления с необходимыми для работы в СКЗИ «Янтарь» инструкциями работнику, зарегистрированному в качестве нового оператора или администратора КС СКЗИ «Янтарь» администратор ОИИ СКЗИ «Янтарь» сообщает начальное значение пароля его учетной записи, которое владелец учетной записи обязан сменить на личный пароль при первом вхождении в СКЗИ «Янтарь».

2.3.2. Отказ в аутентификации (вхождение в СКЗИ «Янтарь») фиксируется в журналах аудита используемой операционной системы СКЗИ «Янтарь».

2.4. Блокирование учетной записи.

2.4.1. Блокирование учетных записей осуществляется администратором ОИИ

СКЗИ «Янтарь» на основании полученной копии соответствующего приказа в случаях:

увольнения пользователя;

перевода пользователя в другое подразделение;

долгосрочного отпуска (более 70 дней).

2.4.2. Администратором безопасности СКЗИ «Янтарь» осуществляется контроль блокирования учетной записи пользователя в СКЗИ «Янтарь».

2.4.3. Блокирование идентификатора внутреннего пользователя осуществляется не позднее 45 дней его неиспользования.

2.4.4. На всех средствах вычислительной техники СКЗИ «Янтарь» осуществляется блокировка учетной записи «Локальный администратор».

Ш. — Организация парольной защиты

3.1. В СКЗИ «Янтарь» реализована двухфакторная аутентификация пользователей с использованием паролей и аппаратных устройств аутентификации, отделенных от СКЗИ «Янтарь» (персональный электронный идентификатор Тоись Метогу).

В СКЗИ «Янтарь» устанавливаются следующие характеристики нароля:

длина пароля — 8 символов, для администратора КС и администратора ОИ - 16 символов;

алфавит пароля - не менее 70 символов;

максимальное количество ввода неправильного пароля до блокировки -— 5 попыток;

блокировка учетной записи после достижения максимального ввода неправильного пароля — 30 минут;

сброс счетчика попыток через — 30 минут;

максимальное временя действия пароля — 40 дней;

минимальное временя действия пароля — 30 дней;

минимальное количество измененных символов при создании новых паролей

5
— 3 символа;

количество хранимых использованных паролей - 6;

максимальное количество неуспешных попыток аутентификации до блокировки учетной записи пользователя -— 5;

при смене пароля, его новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

пароль должен в себя включать буквы нижнего и верхнего регистра в сочетании с цифрами (минимум 1 цифровой символ);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций, слова из словаря, номера телефонов и т.д.), общепринятые сокращения (ЭВМ, ЛВС, ОЗЕВ, $$ и т.д.), а также сочетания символов, соответствующие более чем двум идущим друг за другом клавишам на стандартной клавиатуре в любом направлении;

пароли для входа в СКЗИ «Янтарь» и пароль аутентификации для прохождения программно-аппаратного комплекса «Соболь» не должны совпадать;

защита обратной связи при вводе пароля обеспечивается исключением отображения для пользователя действительного значения пароля (вводимые символы пароля отображаются знаком «*».

3.2. При первичной регистрации оператора или администратора КС в СКЗИ «Янтарь» администратор ОИИ СКЗИ «Янтарь» назначает ему пароль, который предназначен для первоначального входа и должен быть изменен пользователем на личный пароль при первом входе в СКЗИ «Янтарь». Администратор безопасности СКЗИ «Янтарь» выдает пользователю персональный электронный идентификатор Тоисв Мешогу под роспись в журнале «Журнал учета электронных идентификаторов ТоисЬ Метогу, выданных пользователям».

3.3. Отказы в аутентификации (блокирование программно-технического средства или учетной записи) фиксируются в журнале аудита средства защиты информации от несанкционированного доступа и анализируются администратором безопасности СКЗИ «Янтарь» на предмет попыток несанкционированного доступа к СКЗИ «Янтарь». _

3.4. Личный пароль оператора, администратора ОИ или администратора КС является его личной тайной.

3.5. Оператору, администратора ОИ или администратору КС в отношении его личных паролей запрещается:

передавать или сообщать их кому-либо;

использовать автоматическое заполнение или другие возможности запоминания личных паролей, предоставляемые программными средствами СКЗИ «Янтарь»;

записывать их в персональный идентификатор Тоисй Метогу;

сохранять пароль в файловых ресурсах.

3.6. Администратор КС и администратор ОИ должны хранить личные пароли на бумажном носителе в опечатанном виде (в конверте), либо в опечатанном личной печатью пенале. Конверт или пенал с личным паролем хранится в сейфе начальника Отдела режима секретности и безопасности информации.

3.7. Контроль за применением операторами или администраторами КС личных паролей в СКЗИ «Янтарь» осуществляется администратором безопасности.

3.8. В случае компрометации личного пароля, оператор или администратор КС СКЗИ «Янтарь» должен немедленно выполнить внеплановую его смену и доложить о факте компрометации в администратору безопасности.

3.9. Операторы или администраторы КС СКЗИ «Янтарь» должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены © дисциплинарной ответственности за использование паролей, не соответствующих указанным требованиям, а также за разглашение парольной информации.

7
Приложение
к инструкции по организации
назначения (удаления)
учетных записей
пользователям и парольной
защиты в системе
криптографической защиты
информации
автоматизированных систем
Банка России «Янтарь»
Управления Федерального
казначейства по Московской
области
ЗАЯВКА
на допуск к информационным ресурсам АРМ УКС Управления
Прошу сотрудника отдела
Наименование отдела
ФИО, должность, кабинет, телефон
ОИ
в соответствии с приказом Управления о наделении соответствующими правами
1. включить в группу и допустить информационным ресурсам
АРМ УКС Управления.
особенности доступа:
к ресурсу с полномочиями на «чтение», «запись»
ООО чтение», «запись»
«изменение» «выполнение»;
(ненужное зачеркнуть)
к ресурсу с полномочиями на чтение», «запись»
«изменение» «выполнение»
{ненужное зачеркнуть)
ООВ
(обоснование необходимости подключения)
3. обеспечить подключение: CO-BOM / И5В разъемов /
(не нужное зачеркнуть)
ООО
(обоснование необходимости подключения, реквизиты приказа)
Начальник отдела
{Наименование отдела) (Подпись) (Ф.И.О.)

8
Оборотная сторона
ЗАДАНИЕ
на допуск к информационным ресурсам АРМ УКС Управления
Согласовано Персональный идентификатор выдан,
доступ к компьютеру предоставлен

Начальник отдела РСиБИ Администратор безопасности

(Подпись) (Ф.И.О.) (Подпись) (Ф.И.О.)
«_х 20_г. « » 20 Г.

С: «Инструкцией администратора объекта информационной инфраструктуры системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области»;

«Инструкцией операторов ключевой системы и администраторов криптосервера системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» в Управлении Федерального казначейства по Московской области»;

«Порядком обращения с ключевыми документами и ключевыми носителями системы кринтографической защиты информации «Янтарь»;

«Инструкцией по эксплуатации (применению) комплекса средств защиты информации в системе криптографической защиты информации «Янтарь»;

«Общими организационными мерами по обеспечению безопасности информации при } эксплуатации системы криптографической защиты информации «Янтарь» в Управлении Федерального казначейства по Московской области»

«Инструкцией по организации назначения (удаления) учетных записей пользователям и парольной защиты в системе криптографической защиты информации «Янтарь» Управления Федерального казначейства по Московской области» - ознакомлен.

Пользователь " " 20 Г.
(Подпись) (Ф.И.О.
Изменения внесены
Администратор ОИИ
"и " 20 Г
(Подпись) (Ф.И.О.)
Учетная запись получена.
Пользователь " " 20 г.
(Подпись) {Ф.И.О.)
Отметка об удалении учетной записи пользователя в связи с увольнением
Учетная запись удалена
Администратор ИАС
и " 20 Г
(Подпись) (Ф.И.О.)

Приложение № 8
УТВЕРЖДЕН
приказом УФК
по Московской области
от«(0.№ ое 2021т.№ 59,
Перечень мероприятий по проведению контроля в системе криптографической защиты информации автоматизированных систем Банка России «Янтарь»

С целью проведения контроля эксплуатации системы криптографической защиты информации автоматизированных систем Банка России «Янтарь» (далее — СКЗИ «Янтарь») администратором безопасности организуется:

1. Проверка актуальности списка допущенных лиц в помещения с СКЗИ «Янтарь» - раз в 6 месяцев.

2. Проверка актуальности приказов о назначении администраторов безопасности, администраторов криптосервера, администраторов — объекта информационной инфраструктуры и операторов автоматизированного рабочего места управления ключевой системой — раз в 6 месяцев.

3. Проверка правильности хранения ключевых документов и их резервных копий -— раз в 3 месяца.

4. Подробный анализ журналов средств защиты информации СКЗИ «Янтарь» - раз в 3 месяца.

5. Проверка аппаратных журналов СКЗИ «Янтарь» - раз в 6 месяцев.

6. Анализ проведенных проверочных мероприятий по вышеуказанным пунктам и выводы по результатам — последняя рабочая неделя каждого года 6.

Все вышеуказанные мероприятия фиксируются актами о проведении квартального или годового контроля в СКЗИ «Янтарь».