Министерство
сельского хозяйства РФ

ФГБОУ ВО
Кабардино-Балкарский
государственный
аграрный
университет
имени В.М. Кокова

Приказ

02.12.2025г. № 324/О
г. Нальчик

Об обращении со средствами криптографической защиты информации на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России».

В целях исполнения требований приказа ФСБ России от 10 июля 2014 г. № 378 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении 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»

ПРИКАЗЫВАЮ:

1. Назначить Хотова Азамата Лионовича – инженера-программиста ответственным за обеспечение функционирования и безопасности криптографических средств на объекте информатизации – «Информационная система персональных данных для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России» (далее – ИСПДн для подключения к ЗСПД).
2. Утвердить Инструкцию ответственного за обеспечение функционирования и безопасности криптографических средств в ИСПДн для подключения к ЗСПД (Приложение 1).
3. Ответственному за обеспечение функционирования и безопасности криптографических средств в ИСПДн для подключения к ЗСПД ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией ответственного за обеспечение функционирования и безопасности криптографических средств.
4. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (СКЗИ) в ИСПДн для подключения к ЗСПД (Приложение 2).
5. Утвердить инструкцию пользователей СКЗИ (Приложение 3).
6. Ответственному за обеспечение функционирования и безопасности криптографических средств ознакомить под роспись пользователей СКЗИ ИСПДн для подключения к ЗСПД с Инструкцией по обращению с СКЗИ и Инструкцией пользователей СКЗИ.
7. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти инструктаж по правилам работы с СКЗИ.
8. Утвердить Перечень пользователей СКЗИ (Приложение 4).

9. Утвердить форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение 5).

10. Утвердить форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (Приложение 6).

11. Утвердить форму Протокола контрольной проверки информационным системам и ресурсам ИТКИ Минобрнауки России (Приложение 7).

12. Утвердить форму Технического (Аппаратного) журнала СКЗИ (Приложение 8).

13. Приказ довести до сотрудников Учреждения в части касающейся.

14. Контроль за исполнением настоящего приказа оставляю за собой.

Основание: представление инженера-программиста Хотова А.Л., визы: проректора по НР Беровой Д.М., проректора по УР и ЦТ Красовской О.А., проректора по РИ Бозиева Ю.М., начальника ФЭУ Кадыкоева М.А., начальника ЮО Малуховой Р.Х.

Ректор З.Л. Шхагапсоев

Визы:

Проректор по НР Д.М. Берова

Проректор по УР и ЦТ О.А.Красовская

Проректор по РИ Ю.М. Бозиев

Начальник ФЭУ М.А. Кадыкоев

Начальник ЮО Р.Х. Малухова

Приложение 1

к приказу № 324/О от 02.12.2025г.

Инструкция ответственного за обеспечение функционирования и безопасности криптографических средств на объекте информатизации – «Информационная система персональных данных ФГБОЙ ВО Кабардино-Балкарского ГАУ для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за обеспечение функционирования и безопасности криптографических средств (далее – Ответственный) на объекте информатизации – «Информационная система персональных данных **Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова»** для подключения к защищенной сети **передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России** (далее – ИСПДн для подключения к ЗСПД).

Ответственный назначается приказом руководителя Учреждения из числа пользователей криптографических средств, или возлагается на структурное подразделение или должностное лицо (работника), ответственных за защиту информации (обеспечение безопасности информации,
в т. ч. ПДн).

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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 ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152).

2 Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Учреждения в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – сотрудники Учреждения, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

3 Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ в ИСПДн для подключения к ЗСПД необходимо реализовать ряд мероприятий:

– пользователи, которым необходимо получить доступ к работе с СКЗИ, должны быть проинструктированы и обучены правилам работы с СКЗИ;

– учёт лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения защиты информации в ИСПДн для подключения к ЗСПД, осуществлять в Перечне пользователей СКЗИ;

– контроль над реализацией данных мероприятий возлагается на Ответственного за обеспечение функционирования и безопасности криптосредств.

4 Обязанности Ответственного

При решении всех вопросов, связанных с обеспечением безопасности хранения, обработки
и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ в ИСПДн для подключения к ЗСПД.

На Ответственного возлагается проведение следующих мероприятий:

– ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– принятие СКЗИ, эксплуатационной и технической документации к ним, ключевых документов от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– осуществление периодической проверки журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов.

Ответственный обязан:

– не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

– контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

– немедленно уведомлять руководителя Учреждения о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

– незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

– не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

5 Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

– требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;

– обращаться к руководителю Учреждения с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

– инициировать проведение служебных расследований по фактам нарушения в Учреждении порядка обеспечения безопасности хранения, обработки и передачи по каналам связи
с использованием СКЗИ информации ограниченного доступа.

6 Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись
с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

Лист ознакомления
с Инструкцией ответственного за обеспечение функционирования и безопасности криптографических средств
(утверждена приказом № 324/О от 02.12.2025г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

Приложение 2
к приказу № № 324/О от 02.12.2025г.

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России»

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) на объекте информатизации – «Информационная система персональных данных **Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова»** для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России» (далее – ИСПДн для подключения к ЗСПД).

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, в т.ч. ПДн.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на Положении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66; 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 ФАПСИ РФ от 13 июня 2001 г. № 152.

2 Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Учреждения в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – сотрудники Учреждения, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

3 Работа с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, в Учреждении должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под роспись в соответствующих журналах поэкземплярного учета.

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

4 Действия в случае компрометации ключей

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за обеспечение функционирования
и безопасности криптосредств.

К компрометации ключей относятся следующие события:

- утрата носителей ключа;
- утрата иных носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Учреждение (обладатель скомпрометированной информации ограниченного доступа).

5 Обязанности и ответственность лиц, допущенных к работе с СКЗИ

Лица, допущенные к работе с СКЗИ, обязаны:

– не разглашать информацию ограниченного доступа, к которой они допущены;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

– сообщать Ответственному за обеспечение функционирования и безопасности криптосредств о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ;

– немедленно уведомлять Ответственного за обеспечение функционирования и безопасности криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Лица, допущенные к работе с СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала им известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция ответственного за обеспечение функционирования и безопасности криптосредств, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

Лист ознакомления
с Инструкцией по обращению со средствами
криптографической защиты информации
(утверждена приказом № 324/О от 02.12.2025г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

Приложение 3
к приказу № 324/О от 02.12.2025г.

ИНСТРУКЦИЯ
пользователей средств криптографической защиты информации на объекте информатизации – «Информационная система персональных данных Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова» для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России»

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) на объекте информатизации – «Информационная система персональных данных **Федерального государственного бюджетного образовательного учреждения высшего образования «Кабардино-Балкарский государственный аграрный университет имени В.М. Кокова»** для подключения к защищенной сети передачи данных информационным системам и ресурсам ИТКИ Минобрнауки России» (далее – ИСПДн для подключения к ЗСПД).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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 ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152) и «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66.

2 Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Пользователи СКЗИ – работники организации или учреждения, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3 Порядок получения допуска пользователей к работе с СКЗИ

Для работы с СКЗИ привлекаются физические лица, включенные в перечень пользователей СКЗИ, утвержденного соответствующим приказом руководителя организации. Основанием для включения в перечень является Заключение о допуске к самостоятельной работе с СКЗИ. Решение о готовности пользователя к самостоятельной работе с СКЗИ принимает Ответственный за обеспечение функционирования и безопасности криптосредств на основании результатов принятого у пользователя зачета.

Для того чтобы получить Заключение о допуске к самостоятельной работе с СКЗИ, пользователю необходимо выполнить следующее:

1) Самостоятельно ознакомиться с положениями:
   - Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011;
   - Приказа ФАПСИ № 152 от 13.06.2001 «Об утверждении 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»;
   - Настоящей инструкции;
   - Инструкцией о порядке применения средств межсетевого экранирования (при наличии);
   - Инструкцией по обращению со средствами криптографической защиты информации;
   - Эксплуатационной документацией на СКЗИ;
2) Пройти зачет на знание правил работы с СКЗИ;
3) При успешном прохождении тестирования Ответственным за обеспечение функционирования и безопасности криптосредств оформляется Заключение о допуске пользователя к самостоятельной работе с СКЗИ, которое утверждается руководителем организации.

4 Обязанности пользователей СКЗИ

Пользователи СКЗИ обязаны:

- не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- сообщать Ответственному за функционирование и обеспечение безопасности криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять Ответственного за функционирование и обеспечение безопасности криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести
к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Пользователь несет ответственность за то, чтобы на АРМ, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ.

На АРМ, оборудованном СКЗИ, программное обеспечение должно быть лицензионным. При обнаружении на АРМ, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена и организованы мероприятия по анализу
и ликвидации негативных последствий данного нарушения.

Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Не допускается:

– разглашать информацию ограниченного доступа, к которой был допущен пользователь СКЗИ;

– разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;

– выводить ключевую информацию на дисплей и (или) принтер;

– вставлять ключевой носитель в порт АРМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других АРМ;

– записывать на ключевом носителе постороннюю информацию;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за функционирование и обеспечение безопасности криптосредств.

5 Ответственность пользователей СКЗИ

Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей. Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция по обращению с СКЗИ, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

Лист ознакомления
с Инструкцией пользователей средств
криптографической защиты информации
(утверждена приказом № 324/О от 02.12.2025г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

Приложение 4
к приказу № 324/О от 02.12.2025г.

Перечень пользователей СКЗИ

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

Приложение 5
№ 324/О от 02.12.2025г.

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним,
ключевых документов
(форма)

Журнал начат «____» _____ 20__ г.

_____ /Должность/

_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__г.

_____ /Должность/

_____ / ФИО должностного лица /

На _____ листах

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	**Дата подключения (установки) и подписи лиц, произведших подключение (установку)**	**Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ**	**Дата изъятия (уничтожения)**	**Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)**	**Номер акта или расписка об уничтожении**	
9	10	11	12	13	14	15

Приложение 6
к приказу№ 324/О от 02.12.2025г.

АКТ № _____ от «___» _____ 20__ г.
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов
(форма)

Комиссия _____ в составе:
(название организации)
_____
_____
_____
произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования
в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

Ответственный за обеспечение
функционирования и безопасности
криптосредств _____/_____

Члены комиссии:

_____/_____
_____/_____
_____/_____

Приложение 7
к приказу № 324/О от 02.12.2025г.

Протокол
контрольной проверки информационным системам и ресурсам ИТКИ Минобрнауки России
«___» _____ 20___ г.
(форма)

ViPNet Client установлен в_____
наименование подразделения

по адресу:
_____ в соответствии с эксплуатационно-технической документацией, в помещении № _____.

Состав и результаты проверок и контрольных тестов:

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Загрузка ОС с проведением аутентификации пользователя ViPNet.	Загрузка ОС и запуск программного обеспечения ViPNet Client.	
Проверка настроек программного обеспечения.	Настройки программного обеспечения соответствуют требованиям.	
Вход в режим администратора сетевого узла.	Переход программного обеспечения в режим работы администратора сетевого узла.	
Проверка журнала событий ViPNet Client	Отсутствие в журнале событий несанкционированного изменения настроек сетевых фильтров, признаков НСД, аварийных завершений работы программного обеспечения.	
Проверка журнала регистрации IP-пакетов.	Отсутствие в журнале признаков сетевых атак, информации о пропуске IP-пакетов на запрещенные сетевыми фильтрами адреса (протоколы).	
Проверка соединения с видимыми узлами защищенной сети.	Наличие сообщений о доступности сетевых узлов.	
Проверка соединения с видимым узлом защищенной сети, который указан в фильтре, блокирующем прохождение IP- пакетов.	• Наличие сообщений о недоступности сетевого узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых данному узлу.	
Проверка соединения (ping nnn.nnn.nnn.nnn) с открытым узлом с не зарегистрированным адресом.	• Отсутствие ответа от узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых по данному адресу.	
Настройка сетевого фильтра, блокирующего прохождение IP-пакетов в рамках отдельного протокола (например, ICMP) для конкретного узла защищенной сети. Проверка соединения с узлом по данному протоколу	• Отсутствие ответа от узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых в рамках выбранного протокола.	
Настройка сетевого фильтра, блокирующего прохождение IP-пакетов в рамках отдельного протокола (например, UDP) для всех узлов защищенной сети. Проверка соединения с одним из узлов защищенной сети по данному протоколу (например, проверка соединения)	• Наличие сообщений о недоступности сетевого узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых данному узлу.	
Настройка сетевого фильтра, разрешающего прохождение IP-пакетов в рамках отдельного протокола (например, ICMP) для всех узлов открытой сети. Проверка связи с любым открытым узлом по данному протоколу (например, ping).	• Наличие ответа от узла. • Наличие информации в журнале IP-пакетов о прохождении IP-пакетов, передаваемых по данному адресу.	

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Проверка соединения с открытыми узлами с зарегистрированными адресами в рамках разрешенного протокола.	Получение ответа от узлов.	
Проверка соединения с открытыми узлами с зарегистрированными адресами в рамках запрещенного протокола.	Получение ответа от узлов.	
Отправка зашифрованного и подписанного письма адресатам в программе ViPNet Деловая почта.	• Отправка письма. • Получение квитанций о доставке (прочтении).	
Контроль журналов автопроцессинга в программе ViPNet Деловая почта.	Отсутствие сбоев в работе правил автопроцессинга.	

Ответственный за обеспечение функционирования и безопасность СКЗИ

"____"_____ 20___г. _____
подпись

Пользователь

"____"_____ 20___г. _____
подпись

Приложение 8

к приказу № 324/О от 02.12.2025г.

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ СКЗИ (ФОРМА)

Журнал начат «____» _____ 20___ г.

_____ /Должность/

_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20___г.

_____ /Должность/

_____ / ФИО должностного лица /

На _____ листах

20__

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

В настоящем журнале прошнуровано,
пронумеровано и скреплено
___ листов
Ответственный за ведение журнала
_____
_____