Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

ПРИКАЗ

23.05.2024 № 206

Нижний Новгород

Об обращении с шифровальными (криптографическими) средствами защиты информации

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» и «Инструкцией 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 13.06.2001 г. №152, п р и к а з ы в а ю:

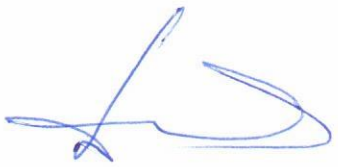
1. Утвердить прилагаемую Инструкцию по обращению с шифровальными (криптографическими) средствами защиты информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее – Инструкция).

2. Утвердить прилагаемый Перечень работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее – Перечень).

3. Ответственному за защиту информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» ознакомить

работников, осуществляющих обработку персональных данных с прилагаемой Инструкцией.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
академик РАН  Г.Г. Денисов

Приложение № 1 к приказу
от "23" .05. 2024 г. № 206

ИНСТРУКЦИЯ
по обращению с шифровальными (криптографическими) средствами защиты информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

1. Основные термины и определения

Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

Ключевой документ - физический носитель определенной структуры, содержащий криптоключи.

Компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

Контролируемая зона - территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

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

Модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

2. Общие положения

2.1 Настоящая Инструкция по обращению с шифровальными (криптографическими) средствами защиты информации (далее – Инструкция) в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук», определяет порядок обращения, размещения, хранения, учета и уничтожения, сертифицированных ФСБ России шифровальных (криптографических) средств защиты информации (далее - СКЗИ), а также ответственных за эксплуатацию СКЗИ.

2.2 Настоящая Инструкция разработана в соответствии с документами:

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России №66 от 9 февраля 2005 года;

– Приказ ФАПСИ при Президенте РФ №152 от 13 июня 2001 года «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».

2.3 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных, и не исключает обязательного выполнения их требований.

3. Ответственные лица

3.1 В Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» ответственность за эксплуатацию сертифицированных СКЗИ, несут:

а) Ответственный за защиту информации**,** на которого возлагаются задачи организации работ по:

- обеспечению корректного и безопасного функционирования СКЗИ;
- обеспечению корректной и безопасной эксплуатации СКЗИ;
- выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;
- контролю работоспособности и соблюдения правил эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ, эксплуатационной и технической документации.

б) Пользователи СКЗИ**,** на которых возлагаются задачи по:

- соблюдению правил корректной и безопасной эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ и ключевых документов, переданных им.

4. Обращение с СКЗИ

4.1 Пользователи СКЗИ допускаются к работе с СКЗИ согласно «Перечню работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»», только после ознакомления под роспись с настоящей Инструкцией и обучения правилам работы с СКЗИ.

4.2 Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации следует использовать СКЗИ.

4.3 При эксплуатации СКЗИ не допускается:

- снимать копии с ключевых документов, за исключением создания резервных копий ключевых документов;
- передавать содержимое документов ключевой информации или передавать сами документы лицам, не имеющим к ним допуска;
- выводить ключи проверки электронной подписи на дисплей, принтер или другие внешние устройства отображения информации;
- записывать на ключевой носитель постороннюю информацию;
- подключать к персональной электронно-вычислительной машине дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;
- работать на персональной электронно-вычислительной машине, если во время его начальной загрузки не проходит встроенный тест, предусмотренный в персональной электронно-вычислительной машине;
- оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;

– несанкционированно устанавливать, создавать и использовать на персональной электронно-вычислительной машине посторонние программы;

– осуществлять несанкционированное вскрытие системных блоков персональной электронно-вычислительной машине.

4.4 Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию, при этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией ограниченного распространения.

4.5 Криптоключи в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

4.6 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственному за защиту информации в информационной системе.

4.7 Ответственный за защиту информации в информационной системе, обязан провести мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ.

5. Размещение технических средств с СКЗИ

5.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

5.2 При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с СКЗИ.

5.3 Требования к режимным помещениям:

– режимные помещения выделяются с учетом размеров контролируемой зоны организации;

– помещения должны быть оборудованы входными дверьми с замками, гарантирующими обеспечение постоянного закрытия дверей помещения на замок и их открытия только для санкционированного прохода;

– помещения должны опечатываться по окончании рабочего дня или должны быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещения;

– окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или должны быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном проникновении в помещение;

– окна помещений, должны быть защищены от просмотра режимных помещений извне.

5.4 Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать ответственному за защиту информации в информационной

системе и пользователям СКЗИ сохранность доверенных им СКЗИ, конфиденциальных документов и сведений, включая ключевую информацию, и свести к минимуму возможность неконтролируемого доступа к ним посторонних лиц.

6. Хранение СКЗИ

6.1 СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы, находящиеся у ответственного за защиту информации в информационной системе и пользователей СКЗИ, должны храниться в месте, исключающем возможность несанкционированного доступа к ним (сейф, шкаф с замком и т.п.).

7. Учет СКЗИ

7.1 Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету ответственным за защиту информации в информационной системе в «Журнале поэкземплярного учета шифровальных (криптографических) средств защиты информации, используемых в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук», эксплуатационной и технической документации к ним, ключевых документов» (Приложение 1).

8. Уничтожение СКЗИ

8.1 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

8.2 Ключевые документы уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

8.3 Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ

8.4 Бумажные и прочие сгораемые ключевые документы, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

8.5 СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-2005.

8.6 Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

9. Обязанности пользователей СКЗИ

9.1 Пользователи СКЗИ обязаны:

– обеспечить конфиденциальность информации о СКЗИ, других мерах защиты;

– точно соблюдать требования настоящей инструкции;

– надежно хранить эксплуатационную и техническую документацию к СКЗИ, ключевые документы, носители дистрибутивов криптосредств;

– сдать СКЗИ эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

– своевременно выявлять и сообщать ответственному за защиту информации в информационной системе о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– немедленно уведомлять ответственного за защиту информации в информационной системе при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей.

10. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

10.1 Государственный контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации осуществляют федеральные органы безопасности.

10.2 В ходе государственного контроля изучаются и оцениваются:

– организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;

– достигнутый уровень криптографической защиты конфиденциальной информации;

– условия использования СКЗИ.

10.3 Ответственный за защиту информации в информационной системе, обязан контролировать выполнение указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ и настоящей Инструкцией.

Приложение 1
к Инструкции по обращению с шифровальными (криптографическими) средствами защиты информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

Журнал поэкземплярного учета шифровальных (криптографических) средств защиты информации используемых в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук», эксплуатационной и технической документации к ним, ключевых документов

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

Инв. № _____

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых докумен-тов	Номера экземпляров (криптографичес-кие номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кото-рым подклю-чены крипто-средства	Дата изъятия (уничто-жения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение № 2 к приказу
от "23" .05. 2024 г. № 206

ПЕРЕЧЕНЬ

работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

№ п/п	Должность
1	Сотрудники, использующие Контру-Экстерн
2	Сотрудники, пользователи ЕГИСМ (иначе ЕИС ГА)
3	Сотрудники, использующие ФИС ФРДО

Лист ознакомления с «Приказом об обращении с шифровальными (криптографическими) средствами защиты информации» от "23".05. 2024 г. № 206		
Занимаемая должность, дата ознакомления	Подпись	И. О. Фамилия
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		