Приложение № 3 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю
Заместитель директора по информационным технологиям,
начальник управления

_____/ И.П. Тарасов/

М.П.

ПОРЯДОК

организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Москва 2020 г.

Содержание

1. Назначение и область применения

Настоящий порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – Порядок), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Порядок определяет условия предоставления и правила пользования услугами ОКЗ, основные организационно-технические мероприятия, направленные на обеспечение работы ОКЗ. Порядок имеет статус локального.

Требования настоящего Порядка распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие автоматизированные и/или информационные системы, в которых хранится, обрабатывается и/или передается по каналам связи с использованием средств криптографической защиты информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну и обязательны для выполнения сотрудниками, исполняющими следующие функциональные роли:

1. Руководитель ООКИ;
2. Аналитик ОКЗ АО «Гринатом»;
3. Администратор безопасности ОКЗ АО «Гринатом»;
4. Руководитель АО «Гринатом»;
5. Начальник Управления информационной безопасности АО «Гринатом»;
6. Руководитель Органа криптографической защиты АО «Гринатом»;
7. Проверяющий.

Настоящий Порядок использует ссылки на следующие документы, необходимые для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

Документ	Статус	Тип документа	Ответствен-ный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных	Действует	Лицензия	Волков С.П.

(криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)			
Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи"	Действует	Федеральный закон	Волков С.П.
Приказ ФАПСИ № 152 от 13.06.2001 г. «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»	Действует	Приказ	Волков С.П.
Приказ ФСБ № 66 от 09.02.2005 г. «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»	Действует	Приказ	Волков С.П.
Приказ ФСБ России от 10.07.2014 г. N 378 «Об утверждении состава и содержания 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»	Действует	Приказ	Волков С.П.

Приказ ГК «Росатом» от 09.01.2019 №1/4-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и ее организациях»	Действует	Требование	Волков С.П.

и является основой для регламентации следующих подпроцессов и процедур:

Подпроцессы:
Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»
Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»
Подпроцесс «Отправка и получение СКЗИ»
Подпроцесс «Учет СКЗИ в ООКИ»
Подпроцесс «Установка и настройка СКЗИ»
Подпроцесс «Генерация ключевой информации»
Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»
Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»
Подпроцесс «Обеспечение функционирования, безопасности и контроля за применением СКЗИ»
Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»
Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»
Подпроцесс «Проверка выполнения требований Порядка»

2. Термины, определения и сокращения

Термин	Определение
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Книга лицевых счетов	Книга регистрации применяющихся Пользователями средств

	криптографической защиты информации, эксплуатационной и технической документации
Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну
Обладатели конфиденциальной информации	Государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица
Орган криптографической защиты	Действующая на постоянной основе рабочая группа из числа сотрудников Управления информационной безопасности
Пользователи СКЗИ	Физические лица, непосредственно допущенные к работе с СКЗИ
Средства криптографической защиты информации (СКЗИ)	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи;

	средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств; ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

	программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств; программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.
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

Сокращение	Расшифровка
АБ	Администратор безопасности ОКЗ АО «Гринатом»

ООКИ	Организация-обладатель конфиденциальной информации
КУЦ	Корпоративный Удостоверяющий центр Госкорпорации «Росатом»
ОКЗ	Орган криптографической защиты АО «Гринатом»
Руководитель ООКИ	Руководитель организации-обладателя конфиденциальной информации
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись

3. Описание процесса

3.1. Цель процесса

Предоставление услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

3.2. Задачи процесса

- Разработка и утверждение схемы организации криптографической защиты информации;
- Формирование комплекта поставки СКЗИ и учет СКЗИ;
- Отправка и получение СКЗИ;
- Учет СКЗИ в ООКИ;
- Установка и настройка СКЗИ;
- Генерация ключевой информации;
- Обучение и допуск Пользователей к самостоятельному использованию СКЗИ;
- Принятие решения о возможности эксплуатации СКЗИ;
- Обеспечение функционирования, безопасности и контроля за применением СКЗИ;
- Расследование фактов нарушений условий использования СКЗИ;
- Вывод из эксплуатации и уничтожение СКЗИ;
- Проверка выполнения требований Порядка.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли
1	Руководитель ООКИ	• Принимает решение о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации; • Принимает решение о допуске пользователей к самостоятельной работе с СКЗИ; • Согласовывает документы, необходимые для получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Принимает решение о прекращении получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Ознакамливается и подписывает документы по результатам проверки и устранению недостатков выполнения требований Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Принимает решение о проведении расследований по фактам нарушения условий использования СКЗИ; • Ознакамливается и подписывает Заключения по результатам расследований фактов нарушения условий использования СКЗИ.

2	Аналитик ОКЗ АО «Гринатом» (далее – Аналитик)	• Разрабатывает и поддерживает в актуальном состоянии схему криптографической защиты информации; • Определяет требования к защищенности различных информационных систем в соответствии с действующей нормативно-методической документацией; • Составляет заключение о возможности эксплуатации СКЗИ; • Формирует комплект поставки СКЗИ; • Учитывает СКЗИ в ОКЗ; • Отправляет СКЗИ в ООКИ.
3	Администратор безопасности ОКЗ АО «Гринатом»	• Подготавливает и согласовывает документы, необходимые для получения услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Получает и учитывает СКЗИ в ООКИ; • Устанавливает, настраивает, проверяет готовность к работе СКЗИ на рабочих местах Пользователей СКЗИ; • Обучает Пользователей СКЗИ. и принимает зачеты; • Осуществляет контроль за правильностью эксплуатации СКЗИ; • Проводит регламентные работы; • Уничтожает выведенные из действия СКЗИ.
4	Руководитель АО «Гринатом»	• Согласовывает Приказ о проведении проверки требований Порядка; • Согласовывает Приказ о проведении расследования условий использования СКЗИ.

5	Начальник Управления информационной безопасности АО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Ознакамливается и подписывает Заключения по результатам расследований фактов нарушения условий использования СКЗИ.
6	Руководитель Органа криптографической защиты АО «Гринатом»	• Согласовывает документы, необходимые для предоставления услуг ОКЗ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну; • Утверждает Заключение комиссии Органа криптографической защиты АО «Гринатом» по результатам расследования фактов нарушения условий использования СКЗИ.
7	Проверяющий	• Подготавливает документы для проведения проверок выполнения требований Порядка; • Осуществляет проверки выполнения требований Порядка; • Отслеживает устранение ООКИ выявленных по результатам проверок недостатков.

3.4. Основные выходы процесса

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
1	2	3	4
1	Приказ о назначении администраторов безопасности и лиц, их замещающих	Предприятие, АО «Гринатом»	Организация
2	Заявление на услугу Администратора безопасности	Предприятие, АО «Гринатом»	Организация
3	Перечень лиц, допускаемых к самостоятельной работе с СКЗИ	Предприятие, АО «Гринатом»	Организация
4	Приказ о назначении прав подписей Пользователей СКЗИ	Предприятие, АО «Гринатом»	Организация
5	Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (с передачей СКЗИ на предприятие)	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
6	Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (без передачи СКЗИ на предприятие)	Предприятие, АО «Гринатом»	Организация
7	Схема организации криптографической защиты информации	АО «Гринатом»	Организация
8	Утвержденная схема организации криптографической защиты информации	АО «Гринатом»	Организация
9	СКЗИ	Предприятие	Организация
10	Книга лицевых счетов	АО «Гринатом»	Организация
11	Доверенность на получение АБ СКЗИ из банка	Предприятие	Организация
12	СКЗИ из банка	Предприятие	Организация
13	Акт повреждения упаковки	АО «Гринатом»	Организация
14	Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
	(для обладателя конфиденциальной информации)		
15	Технический (аппаратный) журнал	Предприятие, АО «Гринатом»	Организация
16	Акт готовности СКЗИ к эксплуатации	Предприятие, АО «Гринатом»	Организация
17	Учтенные ключевые носители	Предприятие	Организация
18	Ключевой носитель с ключевой информацией	Предприятие	Организация
19	Сертификаты	Предприятие	Организация
20	Зарегистрированные сертификаты	Предприятие	Организация
21	Заключение о сдаче зачетов	Предприятие, АО «Гринатом»	Организация
22	Заключение о возможности эксплуатации СКЗИ	Предприятие, АО «Гринатом»	Организация
23	Журнал учета выполнения регламентных работ	Предприятие, АО «Гринатом»	Организация
24	План устранения недостатков с отметками о выполнении	Предприятие, АО «Гринатом»	Организация
25	Акт об уничтожении СКЗИ	Предприятие, АО «Гринатом»	Организация
26	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с	Предприятие, АО «Гринатом»	Организация

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
	ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ		
27	План-график проведения проверок	Предприятие, АО «Гринатом»	Организация
28	Письмо о проведении проверки работ по договору присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств	Предприятие	Организация
29	Сводная таблица по объекту проверки	АО «Гринатом»	Организация
30	Акт проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	Предприятие, АО «Гринатом»	Организация

3.5. Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Отраслевые требования по информационной безопасности №1/4-П-дсп от 09.01.2019	ГК «Росатом»	Корпорация
2	Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (с передачей СКЗИ на предприятие)	Предприятие	Организация
3	Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (без передачи СКЗИ на предприятие)	Предприятие	Организация
4	Скан-копия Приказа о назначении администраторов безопасности и лиц их замещающих	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
5	Заявление на услугу Администратора безопасности	Предприятие	Организация
6	Скан-копия Перечня лиц, допускаемых к самостоятельной работе с СКЗИ	Предприятие	Организация
7	Скан-копия Приказа о назначении прав подписей Пользователей СКЗИ	Предприятие	Организация
8	Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	Предприятие	Организация
9	Скан-копия Заключения о сдаче зачетов	Предприятие	Организация
10	Скан-копия Акта готовности СКЗИ к эксплуатации	Предприятие	Организация
11	Скан-копия Технического (аппаратного) журнала (если он ведется)	Предприятие	Организация
12	Акт об уничтожении СКЗИ	Предприятие	Организация
13	Акт повреждения упаковки	Предприятие	Организация
14	Схема организации криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
15	Утвержденная схема организации криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация
16	СКЗИ	АО «Гринатом»	Организация
17	Сопроводительное письмо к СКЗИ	АО «Гринатом»	Организация
18	Акт приема-передачи банковского СКЗИ	Банк	Организация
19	Доверенность на получение АБ ООКИ СКЗИ из банка	Предприятие	Организация
20	Инструкция по установке СКЗИ	АО «Гринатом»	Организация
21	Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ	АО «Гринатом»	Организация
22	Учтенные ключевые носители	Предприятие	Организация
23	Сертификаты	Банк	Организация
24	Учебные материалы	АО «Гринатом»	Организация
25	Анкеты для опроса пользователей СКЗИ	АО «Гринатом»	Организация
26	Скан-копия Заключения о сдаче зачетов	Предприятие	Организация
27	Заключение о возможности эксплуатации СКЗИ	Предприятие	Организация
28	Эксплуатационная и техническая документация к СКЗИ	АО «Гринатом»	Организация
29	План реализации рекомендаций по	Предприятие	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
	результатам проверки лицензиата ФСБ России АО «Гринатом» в ООКИ		
30	Скан-копия Журнала учета выполнения регламентных работ	Предприятие	Организация
31	Акт уничтожения СКЗИ	Предприятие	Организация
32	Приказ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	АО «Гринатом»	Организация
33	Выписка из схемы криптографической защиты конфиденциальной информации	АО «Гринатом»	Организация
34	Выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом»	АО «Гринатом»	Организация
35	Письмо о проведении проверки в ООКИ	АО «Гринатом»	Организация
36	Сводная таблица по объекту проверки	АО «Гринатом»	Организация
37	Программа проверки организации и обеспечения	АО «Гринатом»	Организация

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
	безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ		
38	Акт проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ	АО «Гринатом»	Организация

3.6. Описание подпроцессов

3.6.1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации»

Руководитель ООКИ:

- Принимает решение о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием

СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в соответствии с Отраслевыми требованиями по информационной безопасности №1/4-П-дсп от 09.01.2019

В случае если принимается решение об обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

- Назначает Приказом АБ и лиц их замещающих (Приложение №4) или использует АБ в рамках связанной услуги GEN.23 «Услуга Администратора безопасности АО «Гринатом» (Приложение №5).
  В рамках услуги GEN.23 АО «Гринатом» предоставляет Администратора безопасности на предприятие, который проводит комплекс работ по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;
- Утверждает Перечень лиц, допускаемых к самостоятельной работе с СКЗИ (Приложение №6);
- Назначает Приказом лиц, имеющих права подписи в системе(ах) (Приложение №7) (в случае если такие права предоставляются);
- Направляет в адрес ОКЗ АО «Гринатом» следующий комплект документов:
  - Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее - Заявление на СКЗИ с передачей СКЗИ на предприятие) (Приложение №8.1), в случае если АО «Гринатом», передает СКЗИ на предприятие или Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее - Заявление на СКЗИ без передачи СКЗИ на предприятие) (Приложение №8.2), в случае если АО «Гринатом» не передает СКЗИ на предприятие;
  - Скан-копию Приказа о назначении АБ и лиц их замещающих или Заявление на услугу Администратора безопасности;
  - Скан-копию Перечня лиц, допускаемых к самостоятельной работе с СКЗИ;
  - Скан-копию Приказа о предоставлении прав подписей в системе(ах).

Исходящая информация поступает в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

В случае если принимается решение о выводе СКЗИ из эксплуатации:

- Принимает решение о выводе СКЗИ из эксплуатации.

Исходящая информация поступает в подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ».

3.6.2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»

Входящая информация поступает из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации» или из подпроцесса «Вывод из эксплуатации и уничтожение СКЗИ».

Аналитик:

- Разрабатывает «Схему организации криптографической защиты конфиденциальной информации» (далее – Схема) (Приложение №9) на основании данных, указанных в Заявлении на СКЗИ (с передачей СКЗИ на предприятие), Заявления на СКЗИ (без передачи СКЗИ на предприятие), скан-копии Приказа о назначении АБ и лиц их замещающих или Заявления на услугу Администратора безопасности, скан-копии Перечня лиц, допускаемых к самостоятельной работе с СКЗИ, скан-копии Приказа о предоставлении прав подписей Пользователей СКЗИ, скан-копии Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации), скан-копии Заключения о сдаче зачетов, скан-копии Технического (аппаратного) журнала, скан-копии Акта готовности СКЗИ к эксплуатации, Акта об уничтожении СКЗИ, Акта повреждения упаковки.

Начальник управления информационной безопасности АО «Гринатом»:

- Утверждает Схему.

Если Аналитику пришла информация из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации», то исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ».

Если Аналитику пришла информация из подпроцесса «Вывод из эксплуатации и уничтожение СКЗИ», то процесс взаимодействия ОКЗ и ООКИ завершается.

Исходящая информация поступает в подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ» или в конец процесса.

3.6.3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ»

Входящая информация поступает из подпроцесса «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

Аналитик:

- Формирует комплект поставки СКЗИ;
- Учитывает СКЗИ в Книге лицевых счетов ОКЗ АО «Гринатом» (Приложение №10).

Если СКЗИ получаются из банка, то комплект поставки не формируется Аналитиком.

Исходящая информация поступает в подпроцесс «Отправка и получение СКЗИ».

3.6.4. Подпроцесс «Отправка и получение СКЗИ»

Входящая информация поступает из подпроцесса «Формирование комплекта поставки СКЗИ и учет СКЗИ».

Способы доставки СКЗИ:

- фельдъегерской (в том числе ведомственной) связью;
- доверенным лицом (необходима доверенность по форме Приложения №11);
- АБ.

Доставка осуществляется при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ во время доставки.

Пересылка эксплуатационной и технической документации СКЗИ организуется и производится Аналитиком заказным или ценным почтовым отправлением.

Аналитик:

- Помещает СКЗИ в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.
  На упаковках указывает АБ, для которых эти упаковки предназначены. Упаковки опечатывает таким образом, чтобы исключить возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.
  Помещает во внешнюю упаковку при предъявлении фельдсвязью дополнительных требований;
- Подготавливает сопроводительное письмо (Приложение №12), в котором указывает, что посылается и в каком количестве, учетные номера изделий и/или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывает в одну из упаковок.

АБ:

- Получает упаковку с СКЗИ;

- Составляет и направляет в адрес ОКЗ АО «Гринатом» акт повреждения упаковки (Приложение №13) (*в случае, если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому*), после чего ожидает указаний от ОКЗ АО «Гринатом» о дальнейшем применении СКЗИ (*в случае составления акта повреждения упаковки*).

АБ (в случае если СКЗИ получаются из банка, а также других УЦ, данные работы входят в состав услуги GEN.43):

- Запрашивает и заполняет актуальные шаблоны доверенностей;
- Запрашивает и заполняет актуальные шаблоны документов на получение первичной ключевой информации;
- Согласовывает документы на первичную ключевую информацию с поддержкой банка, УЦ или ИС, а также ответственными со стороны ООКИ;
- Выезжает в УЦ для получения ключа ЭП;
- Подписывает при получении СКЗИ или ЭП акт приема-передачи, по форме установленной банком, УЦ или другой организацией.

Исходящая информация поступает в подпроцесс «Учет СКЗИ в ООКИ» или в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации» (*в случае, если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому).*

3.6.5. Подпроцесс «Учет СКЗИ в ООКИ»

Входящая информация поступает из подпроцесса «Отправка и получение СКЗИ».

АБ:

- Учитывает СКЗИ в «Журнале поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)» (далее – Журнал учета (для обладателя конфиденциальной информации) (Приложение №14);
- Отправляет подтверждение о получении СКЗИ в ОКЗ АО «Гринатом» в соответствии с порядком, указанным в сопроводительном письме.

Все полученные АБ экземпляры СКЗИ, эксплуатационная и техническая документация к ним должны быть выданы под расписку в Журнале учета (для обладателя конфиденциальной информации) Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

В случае если СКЗИ получаются из банка, подтверждение в получении СКЗИ в ОКЗ АО «Гринатом» не отправляется.

Исходящая информация поступает в подпроцесс «Установка и настройка СКЗИ».

3.6.6. Подпроцесс «Установка и настройка СКЗИ»

Входящая информация поступает из подпроцесса «Учет СКЗИ в ООКИ».

АБ:

- Устанавливает и настраивает СКЗИ в соответствии с Инструкцией по установке СКЗИ (поставляется в комплекте к СКЗИ);
- Учитывает факт установки и настройки СКЗИ в Журнале учета (для обладателя конфиденциальной информации);
- Проверяет готовность АРМ с установленным СКЗИ на соответствие «Отраслевым требованиям по информационной безопасности №1/4-П-дсп» от 09.01.2019 и «Порядку разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ» (Приложение №15), делает запись об опечатывании технических средств СКЗИ в Техническом (аппаратном) журнале (Приложение №16).
  Технический (аппаратный) журнал ведется в случае ввода ключевой информации на весь срок эксплуатации.
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17).

Исходящая информация поступает в подпроцесс «Генерация ключевой информации».

3.6.7. Подпроцесс «Генерация ключевой информации»

Входящая информация поступает из подпроцесса «Установка и настройка СКЗИ».

При получении СКЗИ от ОКЗ АО «Гринатом» генерация ключевой информации не производится.

АБ (в случае если СКЗИ получаются из банка, а также других УЦ, данные работы входят в состав услуги GEN.43):

- Ставит на учет носители информации в качестве ключевых;
- Подписывает запрос на генерацию ключевых документов у пользователя СКЗИ и руководителя ООКИ;
- Передает запрос на генерацию ключа на бумажном носителе в бухгалтерию ООКИ для проставления оттиска печати (в случае необходимости);
- Отправляет в ИС запрос на генерацию ключевой информации подписанта;
- Принимает ключ на АРМ пользователя СКЗИ;
- Производит генерацию технологического ключа (в случае необходимости);

- Учитывает факт генерации и передачи Пользователям в Журнале поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);
- Отправляет сертификаты в ИС;
- Делает отметку в Журнале учета (для обладателя конфиденциальной информации) о сроках действия сертификата;
- Передает данные о ключевых документах в ОКЗ.

Исходящая информация поступает в подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ».

3.6.8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»

Входящая информация поступает из подпроцесса «Генерация ключевой информации».

Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.

АБ:

- Осуществляет обучение Пользователей СКЗИ, применяя учебные материалы (Приложение №18);
- Проводит опрос Пользователей СКЗИ по окончании обучения, используя Анкеты для опроса пользователей СКЗИ (Приложение №19) и заполняет Заключение о сдаче зачетов (Приложение №20);
- Направляет в адрес ОКЗ АО «Гринатом» следующий комплект документов:
  - скан-копию Журнала учета (для обладателя конфиденциальной информации);
  - скан-копию Технического (аппаратного) журнала (*в случае если он ведется*);
  - скан-копию Заключения о сдаче зачетов;
  - скан-копию Акта готовности СКЗИ к эксплуатации.

Исходящая информация поступает в подпроцесс «Принятие решения о возможности эксплуатации СКЗИ».

3.6.9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»

Входящая информация поступает из подпроцесса «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ».

Аналитик:

- Составляет Заключение о возможности эксплуатации СКЗИ (Приложение №21) на основании следующих полученных от ООКИ документов:

- Заявления на СКЗИ (с передачей СКЗИ на предприятие);
- Заявления на СКЗИ (без передачи СКЗИ на предприятие);
- Скан-копии Приказа о назначении администраторов безопасности и лиц их замещающих или Заявления на услугу Администратора безопасности;
- Скан-копии Перечня лиц, допускаемых к самостоятельной работе с СКЗИ;
- Скан-копии Приказа о назначении прав подписей пользователей СКЗИ;
- Скан-копии Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);
- Скан-копии Технического (аппаратного) журнала *(если он ведется)*;
- Скан-копии Заключения о сдаче зачетов;
- Скан-копии Акта готовности СКЗИ к эксплуатации.

- Отправляет Заключение о возможности эксплуатации СКЗИ в ООКИ.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

3.6.10. Подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ»

Входящая информация поступает из подпроцесса «Принятие решения о возможности эксплуатации СКЗИ» или из подпроцесса «Проверка выполнения требований Порядка».

Функционирование и безопасность применения СКЗИ обеспечивается в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

Оригиналы выданных сертификатов соответствия требованиям безопасности находятся в ОКЗ АО «Гринатом», копии находятся в ООКИ.

АБ (если проводятся регламентные работы):

- Дополнительно к проверке порядка использования СКЗИ проводит регламентные работы с СКЗИ не реже одного раза в 6 месяцев, о чем делает отметки в Журнале учета выполнения регламентных работ (Приложение №22). Перечни регламентных работ указаны в формулярах на СКЗИ.

АБ (если СКЗИ получены из банка, работы входят в состав услуги GEN.43):

- Дополнительно к проверке порядка использования СКЗИ отслеживает сроки действия ключевой информации Пользователей с помощью Журнала учета (для обладателя конфиденциальной информации). В

случае если срок действия ключевой информации истекает, проводит процедуру генерации новой ключевой информации Пользователей;
- Отслеживает сроки действия доверенностей;
- Ведет реестр ключей, доверенностей и АРМ;
- Предоставляет информацию о сроках действия ключей и доверенностей на подписантов по запросам пользователей;
- Предоставляет информацию для паспорта рабочего места.

АБ (если входящая информация поступает из подпроцесса «Принятие решения о возможности эксплуатации СКЗИ»):

- Осуществляет проверку порядка использования СКЗИ в соответствии с эксплуатационной и технической документацией с периодичностью не реже 1-го раза в год. В состав проверки входит как минимум:
  - соответствие номеров СКЗИ данным в книгах и журналах учета СКЗИ;
  - наличие носителей ключевой информации и их соответствие данным, указанным в книгах и журналах учета СКЗИ;
  - соответствие настроек системного ПО, СКЗИ и мер физической защиты СКЗИ требованиям документации к СКЗИ;
  - наличие носителей ключевой информации и их соответствие данным, указанным в книгах и журналах учета СКЗИ.
- Проставляет отметки в Техническом (аппаратном) журнале *(в случае, если он ведется)*;
- Составляет Акт готовности СКЗИ к эксплуатации (Приложение №17);
- Направляет в ОКЗ АО «Гринатом»:
  - скан-копию Технического (аппаратного) журнала *(если он ведется)*;
  - скан-копию Акта готовности СКЗИ к эксплуатации;
  - скан-копию Журнала учета выполнения регламентных работ *(если регламентные работы проводятся)*.

АБ (если входящая информация поступает из подпроцесса «Проверка выполнения требований Порядка»):

- Устраняет недостатки, выявленные в ходе проверки выполнения требований Порядка;
- Проставляет отметки об устранении недостатков в Плане устранения недостатков, выявленных в ходе проверки выполнения требований Порядка;
- Направляет в ОКЗ АО «Гринатом» План устранения недостатков, выявленных в ходе проверки выполнения требований Порядка, с отметками об устранении.

Аналитик/Проверяющий:

- Обрабатывают полученные документы от АБ.

В случае, если в результате обработки полученных документов выявятся факты нарушений условий использования СКЗИ, то может быть инициировано расследование.

Исходящая информация поступает в подпроцесс «Генерация ключевой информации», в подпроцесс «Расследование фактов нарушений условий использования СКЗИ» или в начало подпроцесса «Обеспечение функционирования, безопасности и контроля за применением СКЗИ».

3.6.11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»

Входящая информация поступает из подпроцесса «Обеспечение функционирования, безопасности и контроля за применением СКЗИ».

Подпроцесс «Расследование фактов нарушений условий использования СКЗИ» описан в документе «Порядок проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом» (Приложение №23).

Расследование фактов нарушения условий использования СКЗИ может быть инициировано со стороны ООКИ, со стороны АО «Гринатом» или ФСБ России.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

3.6.12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»

Входящая информация поступает из подпроцесса «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации».

Руководитель ООКИ:

- Принимает решение о выводе СКЗИ из эксплуатации;

АБ:

- Изымает СКЗИ из аппаратных средств, с которыми они функционировали. При этом СКЗИ считается изъятым из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и он полностью отсоединен от аппаратных средств;
- Уничтожает СКЗИ на месте.
  В случае если ООКИ отказывается от услуги CLB.18, то уничтожение СКЗИ производится по акту (уничтожение производится комиссионно в составе не менее двух АБ, Приложение № 24). В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая

запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых СКЗИ, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. При этом в Журнале учета (для обладателя конфиденциальной информации) в графах об изъятии и уничтожении СКЗИ указываются реквизиты Акта уничтожения.

Уничтожение путем физического уничтожения или путем стирания (разрушения), исключающего возможность их использования, а также восстановления. Непосредственные действия по уничтожению конкретного типа СКЗИ регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями ОКЗ АО «Гринатом».

Бумажные и прочие сгораемые материалы, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью шредеров.

СКЗИ должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то СКЗИ должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

- В случае если ООКИ не отказываются от услуги CLB.18, то уничтожение СКЗИ сопровождается отметками в Журнале учета (для обладателя конфиденциальной информации) об изъятии и уничтожении СКЗИ, при этом Акт уничтожения не составляется;
- Направляет в адрес ОКЗ АО «Гринатом» следующие документы:
  - скан-копию Журнала учета (для обладателя конфиденциальной информации);
  - Акт об уничтожении СКЗИ.

Не реже одного раза в год АБ должны направлять в ОКЗ АО «Гринатом» письменные отчеты об уничтоженных СКЗИ. ОКЗ АО «Гринатом» вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Исходящая информация поступает в подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации».

3.6.13.Подпроцесс «Проверка выполнения требований Порядка».

Руководитель АО «Гринатом»:

- Утверждает Приказ о проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих

государственную тайну в ООКИ (Приложение №25) и План-график проведения проверок (Приложение №26).

Проверяющий:

- Подготавливает и отправляет письмо Руководителю ООКИ о проведении проверки работ по договору присоединения на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (далее – Информационное письмо о проведении проверки, Приложение №27);
- Изучает материалы по объекту проверки:
  - выписку из Схемы организации криптографической защиты конфиденциальной информации (перечень СКЗИ, выданных ОКЗ на предприятие);
  - выписку из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом» (перечень сертификатов ключей проверки электронной подписи, выданных на предприятие).
- Заполняет Сводную таблицу по объекту проверки (Приложение №28);
- Проводит проверку организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ в соответствии с Программой проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ (далее – Программа проверки, Приложение №29) и Сводной таблицей по объекту проверки;
- Подготавливает, подписывает и отправляет в адрес Руководителя ООКИ 2 экземпляра Акта проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в ООКИ (далее – Акт проверки, Приложение №30).

Руководитель Органа криптографической защиты АО «Гринатом»:

- Согласовывает Информационное письмо о проведении проверки;
- Согласовывает Программу проверки;
- Утверждает Акт проверки.

Начальник Управления информационной безопасности АО «Гринатом»:

- Согласовывает Программу проверки;
- Ознакамливается под роспись с Актом проверки.

Руководитель ООКИ:

- Ознакамливается под расписку с Актом проверки;
- Составляет и направляет в адрес Руководителя ОКЗ АО «Гринатом»:
  - План реализации рекомендаций по результатам проверки лицензиата ФСБ России АО «Гринатом» в ООКИ (далее – План устранения недостатков, Приложение №31);
  - Один экземпляр подписанного Акта проверки.

В случае если условия использования СКЗИ не нарушены, то Руководитель ООКИ возвращает только один экземпляр подписанного Акта проверки, План устранения недостатков не составляется.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ».

4. Нормативные ссылки

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ ФАПСИ № 152 от 13.06.2001г. «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»;
- Приказ ФСБ № 66 от 09.02.2005г «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ ФСБ России от 10.07.2014 г. N 378 «Об утверждении состава и содержания 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»;
- Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи";
- Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";
- Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных

(криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- Отраслевые требования по информационной безопасности №1/4-П-дсп от 09.01.2019;
- Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

5. Порядок внесения изменений

Внесение изменений (дополнений) в Порядок, а также в приложения к нему, производится посредством утверждения новой редакции Порядка.

6. Контроль и ответственность

6.1 Порядок обязаны соблюдать все следующие участники процесса:

Руководитель ООКИ;
Аналитик ОКЗ АО «Гринатом»;
Администратор безопасности ОКЗ АО «Гринатом»;
Руководитель АО «Гринатом»;
Начальник Управления информационной безопасности АО «Гринатом»;
Начальник Отдела криптографической защиты АО «Гринатом»;
Проверяющий.

6.2. Ответственность работников за несоблюдение требований Порядка.

За несоблюдение Порядка ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством.

7. Перечень приложений

Приложение №1.	Матрица ответственности.
Приложение №2.	Схема процесса.
Приложение №3.	Дополнительные выходы и дополнительные входы.
Приложение №4.	Форма приказа о назначении Администраторов безопасности и лиц их замещающих
Приложение №5.	Форма Заявления на услугу Администратора безопасности
Приложение №5.1.	Форма Заявления на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя
Приложение №6.	Перечень лиц, допускаемых к самостоятельной работе с СКЗИ
Приложение №7.	Форма Приказа о предоставлении прав подписей
Приложение №8.1.	Заявление на СКЗИ (с передачей СКЗИ)
Приложение №8.2.	Заявление на СКЗИ (без передачи СКЗИ)
Приложение №9.	Схема организации криптографической защиты конфиденциальной информации (шаблон)
Приложение №10.	Книга лицевых счетов
Приложение №11.	Доверенность доверенного лица на получение СКЗИ в ОКЗ
Приложение №12.	Сопроводительное письмо к СКЗИ
Приложение №13.	Акт повреждения упаковки
Приложение №14.	Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Приложение №15.	Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ
Приложение №16.	Технический (аппаратный) журнал
Приложение №17.	Акт готовности СКЗИ к эксплуатации
Приложение №18.	Учебные материалы
Приложение №19.	Анкета для опроса Пользователей
Приложение №20.	Заключение о сдаче зачетов
Приложение №21.	Заключение о возможности эксплуатации СКЗИ
Приложение №22.	Журнал выполнения регламентных работ
Приложение №23.	Порядок проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом»
Приложение №24.	Акт уничтожения СКЗИ
Приложение №25.	Приказ о проведении проверки
Приложение №26.	План-график проведения проверок
Приложение №27.	Информационное письмо о проведении проверки

Приложение №28. Сводная таблица по объекту проверки
Приложение №29. Программа проверки
Приложение №30. Акт проверки
Приложение №31. План устранения недостатков

Приложение №1. Матрица ответственности

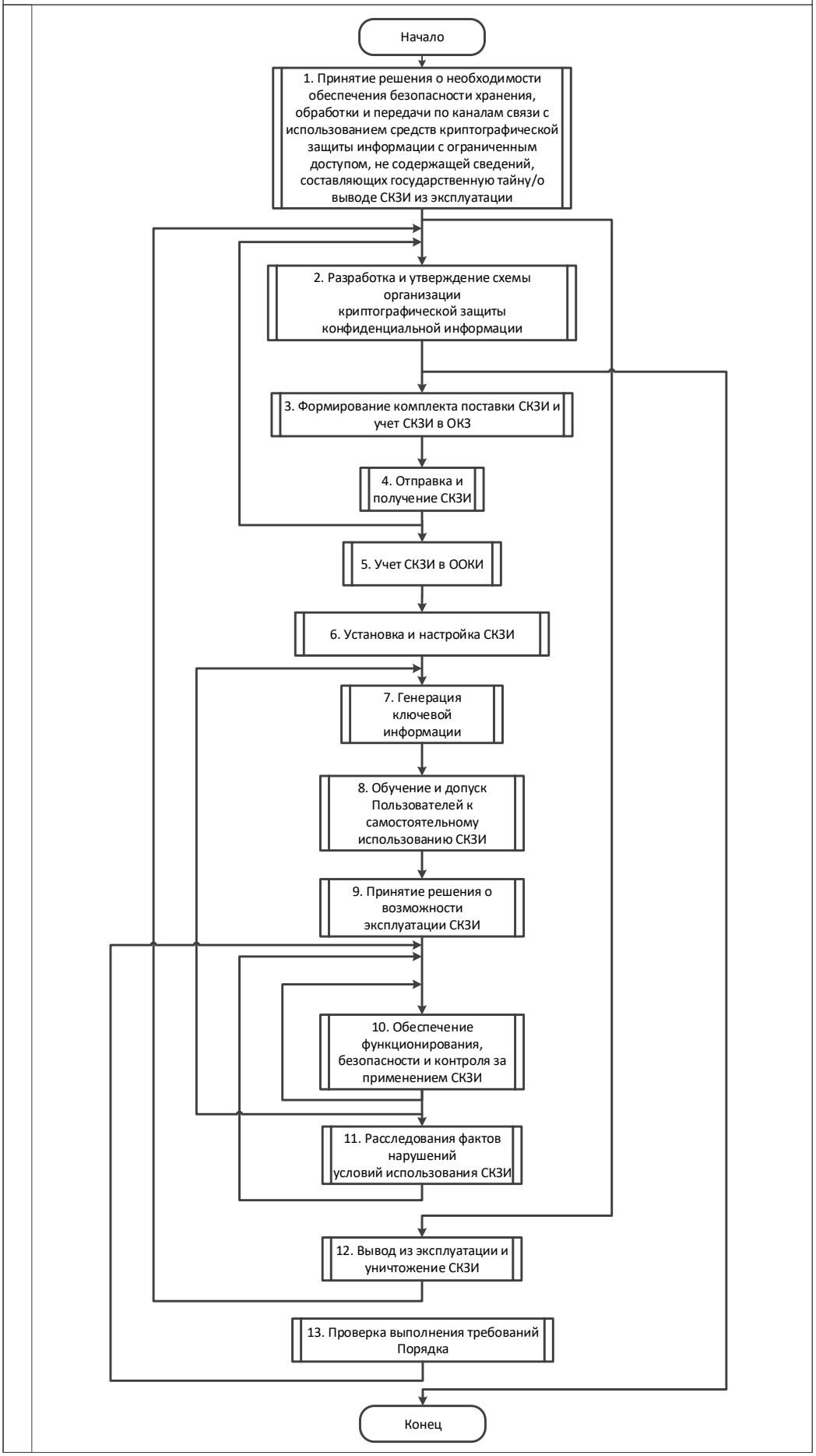
Подпроцессы в составе процесса	Участники процесса						
	Руководитель ООКИ	Аналитик»	АБ	Начальник Управления информационной безопасности АО «Гринатом»	Руководитель Органа криптографической защиты АО «Гринатом»	Руководитель АО «Гринатом»	Проверяющий
Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Утв.						
Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»		О		Утв.			
Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ»		О					
Подпроцесс «Отправка и получение СКЗИ»		О	О				
Подпроцесс «Учет СКЗИ в ООКИ»		Инф.	О				
Подпроцесс «Установка и настройка СКЗИ»		Инф.	О				
Подпроцесс «Генерация ключевой информации»		Инф.	О				
Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»		Инф.	О				
Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»		О	Инф.				
Подпроцесс «Обеспечение функционирования и безопасности и контроля за применением СКЗИ»		Инф.	О				
Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»	Инф.			Инф.	О		О
Подпроцесс «Вывод из эксплуатации и уничтожения СКЗИ»	Утв.	Инф.	О				
Подпроцесс «Проверка выполнения требований Порядка»	О		О	О	О	Утв.	О

Сокра-щение	Название роли	Определение	Исполнитель Роли

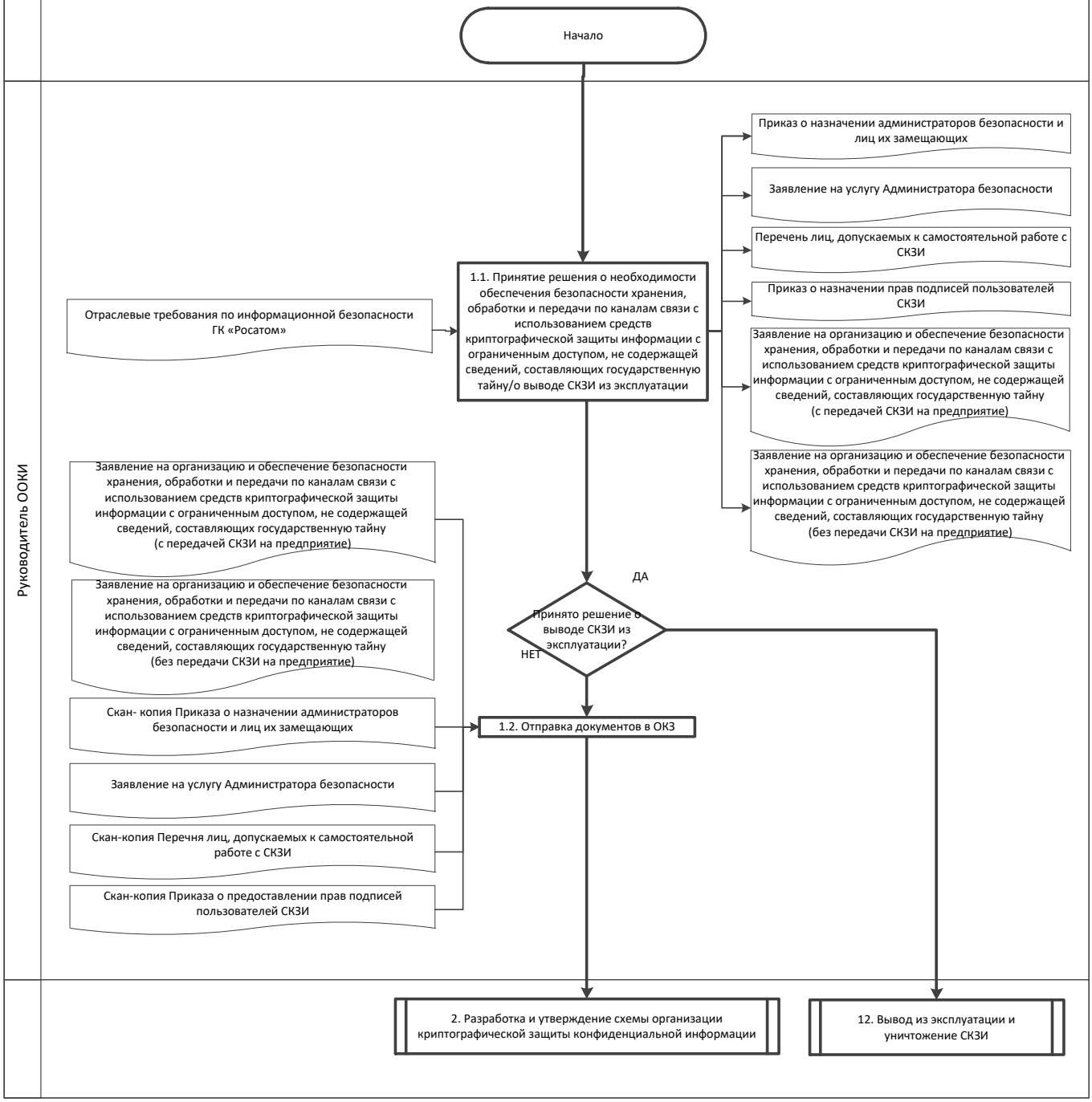
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/ Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	Коллегиальные органы (Наблюдательный совет, Правление и прочие) Генеральный директор Корпорации, Руководители Корпорации /Дивизионов/Организаций
С	Согласовывающий	Согласовывает /одобряет результаты подпроцесса/процедуры для дальнейшего принятия решений	Коллегиальные органы Руководители Корпорации/ Дивизионов/ Организаций
Э	Экспертирующий	Осуществляет экспертизу по подпроцессу/процедуре	Коллегиальные органы Структурное подразделение Корпорации/Дивизиона/ Организации
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации Коллегиальные органы

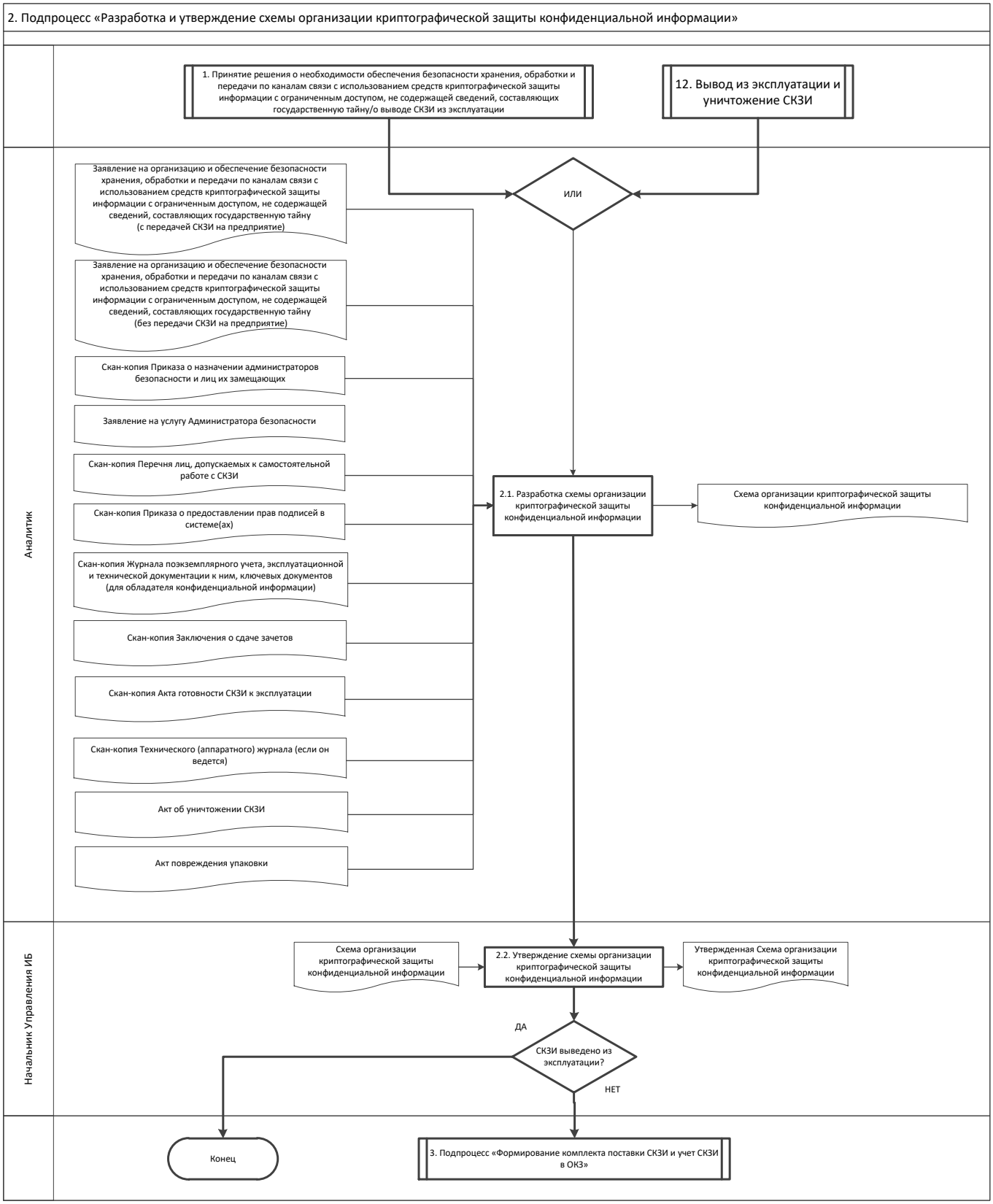
Приложение №2. Схема процесса

Процесс «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

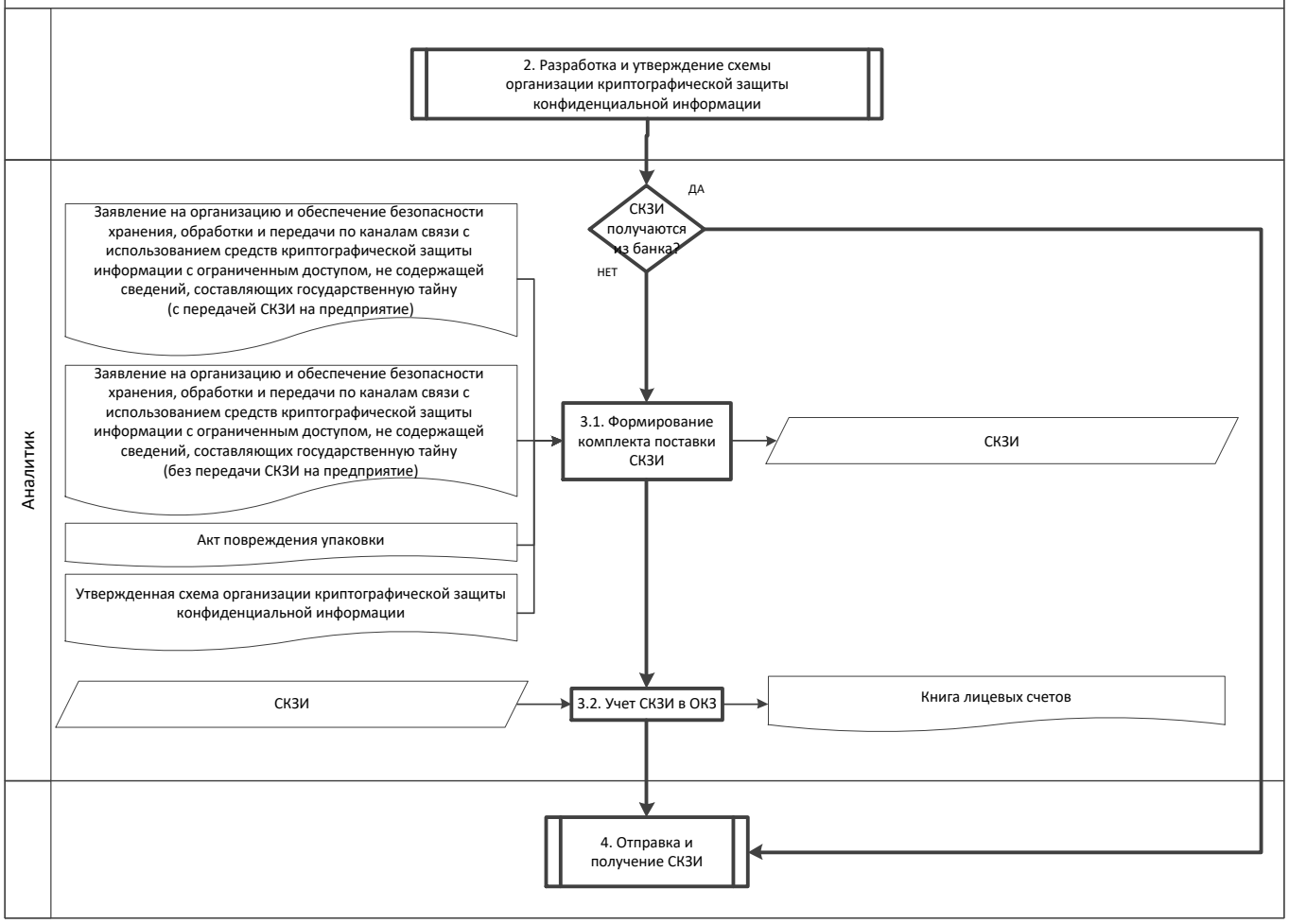


1. Подпроцесс «Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации»

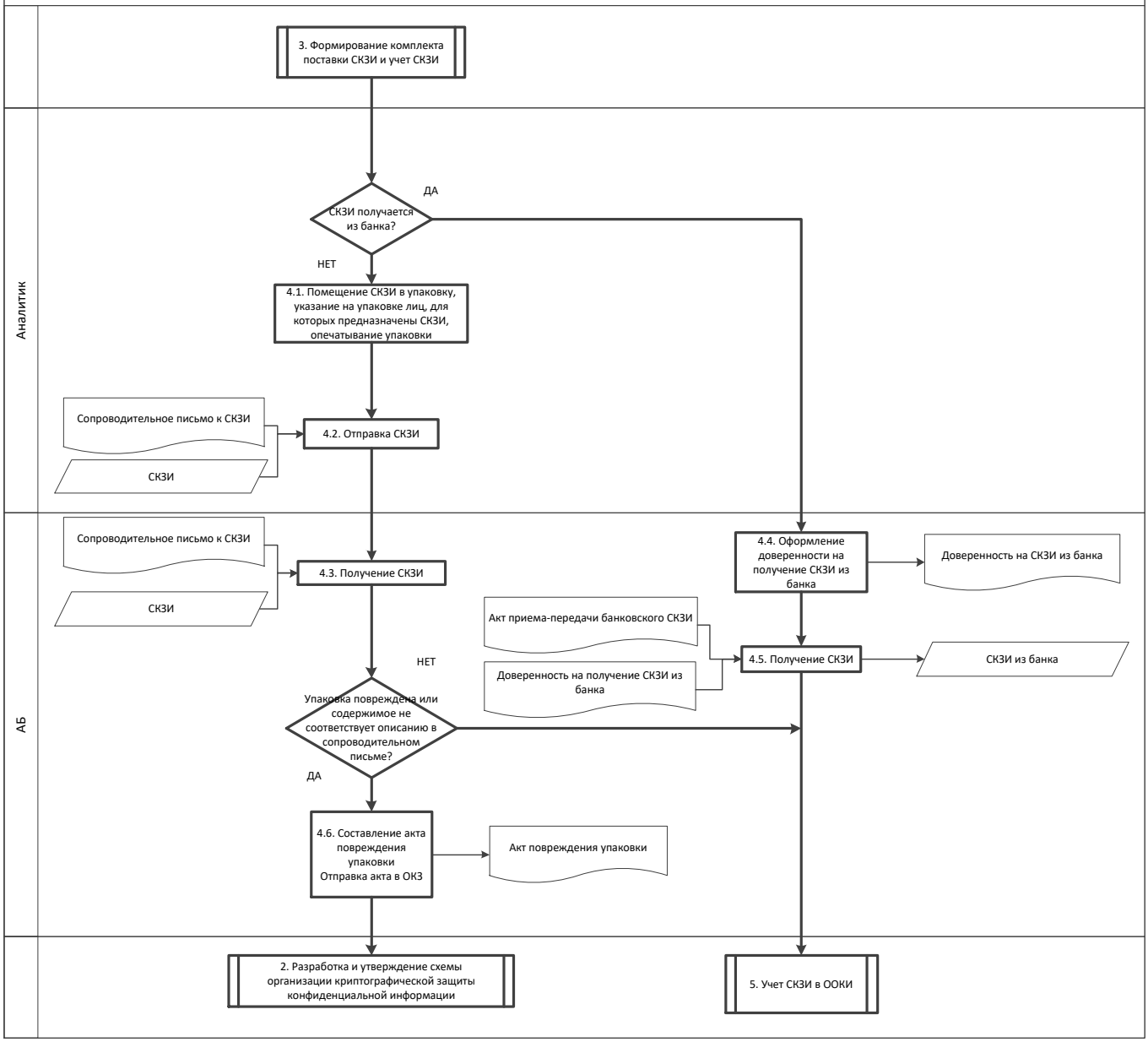



2. Подпроцесс «Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации»
Аналитик
Начальник Управления ИБ
1. Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации
12. Вывод из эксплуатации и уничтожение СКЗИ
ИЛИ
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (с передачей СКЗИ на предприятие)
Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (без передачи СКЗИ на предприятие)
Скан-копия Приказа о назначении администраторов безопасности и лиц их замещающих
Заявление на услугу Администратора безопасности
Скан-копия Перечня лиц, допускаемых к самостоятельной работе с СКЗИ
Скан-копия Приказа о предоставлении прав подписей в системе(ах)
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Скан-копия Заключения о сдаче зачетов
Скан-копия Акта готовности СКЗИ к эксплуатации
Скан-копия Технического (аппаратного) журнала (если он ведется)
Акт об уничтожении СКЗИ
Акт повреждения упаковки
2.1. Разработка схемы организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
Схема организации криптографической защиты конфиденциальной информации
2.2. Утверждение схемы организации криптографической защиты конфиденциальной информации
Утвержденная Схема организации криптографической защиты конфиденциальной информации
ДА
СКЗИ выведено из эксплуатации?
НЕТ
Конец
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»

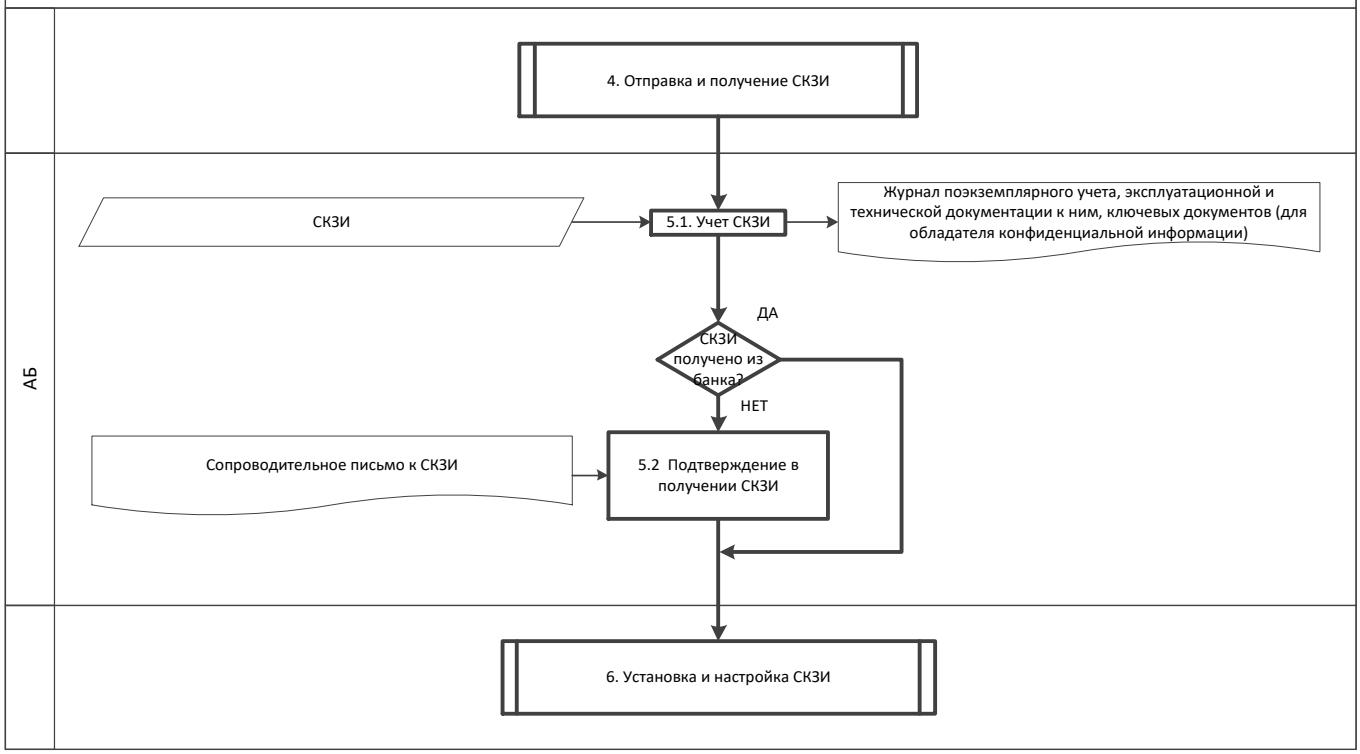
3. Подпроцесс «Формирование комплекта поставки СКЗИ и учет СКЗИ в ОКЗ»



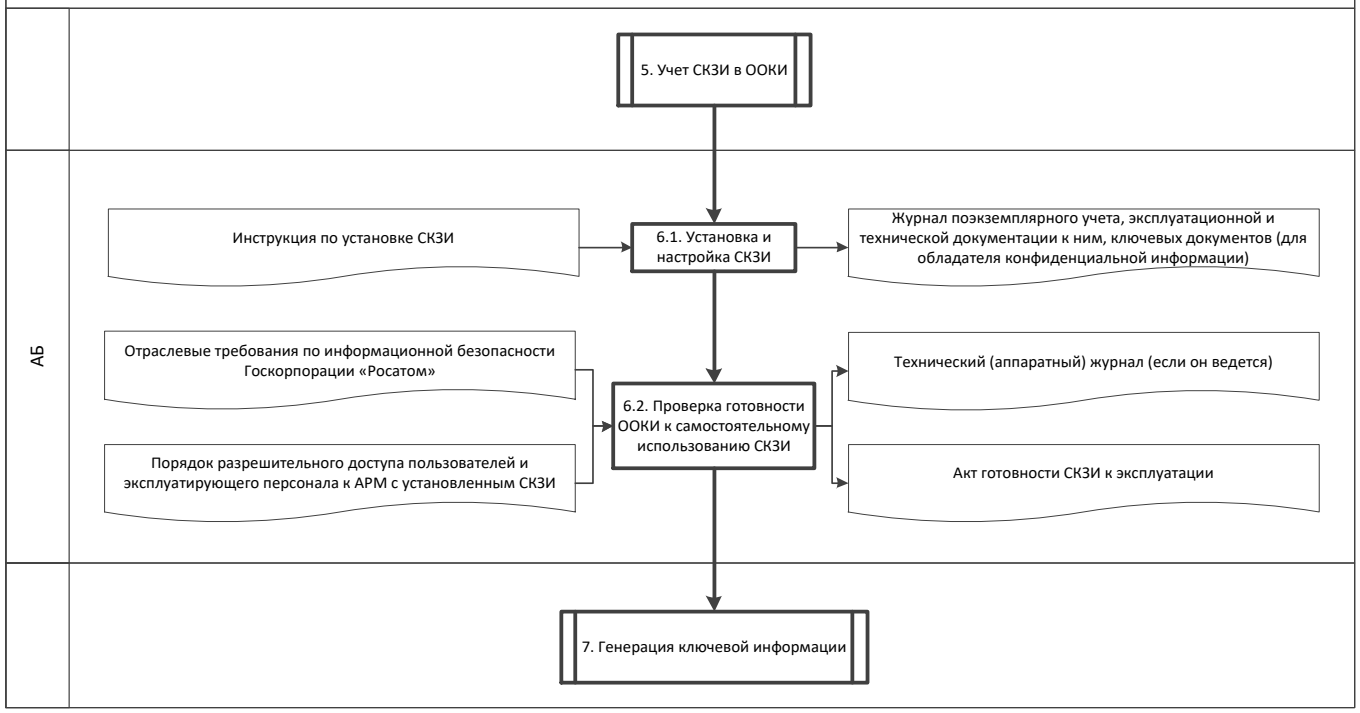
4. Подпроцесс «Отправка и получение СКЗИ»



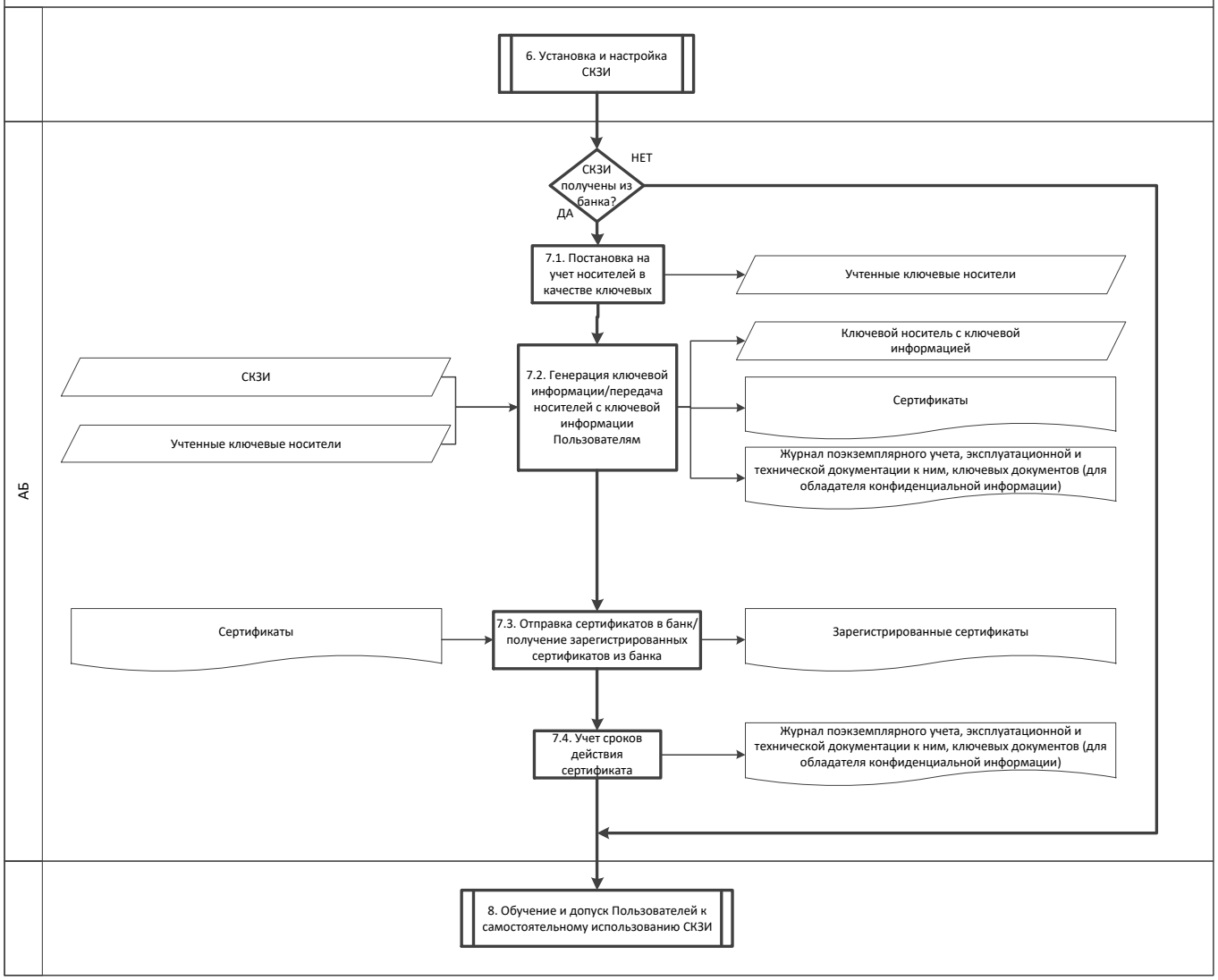
5. Подпроцесс «Учет СКЗИ в ООКИ»



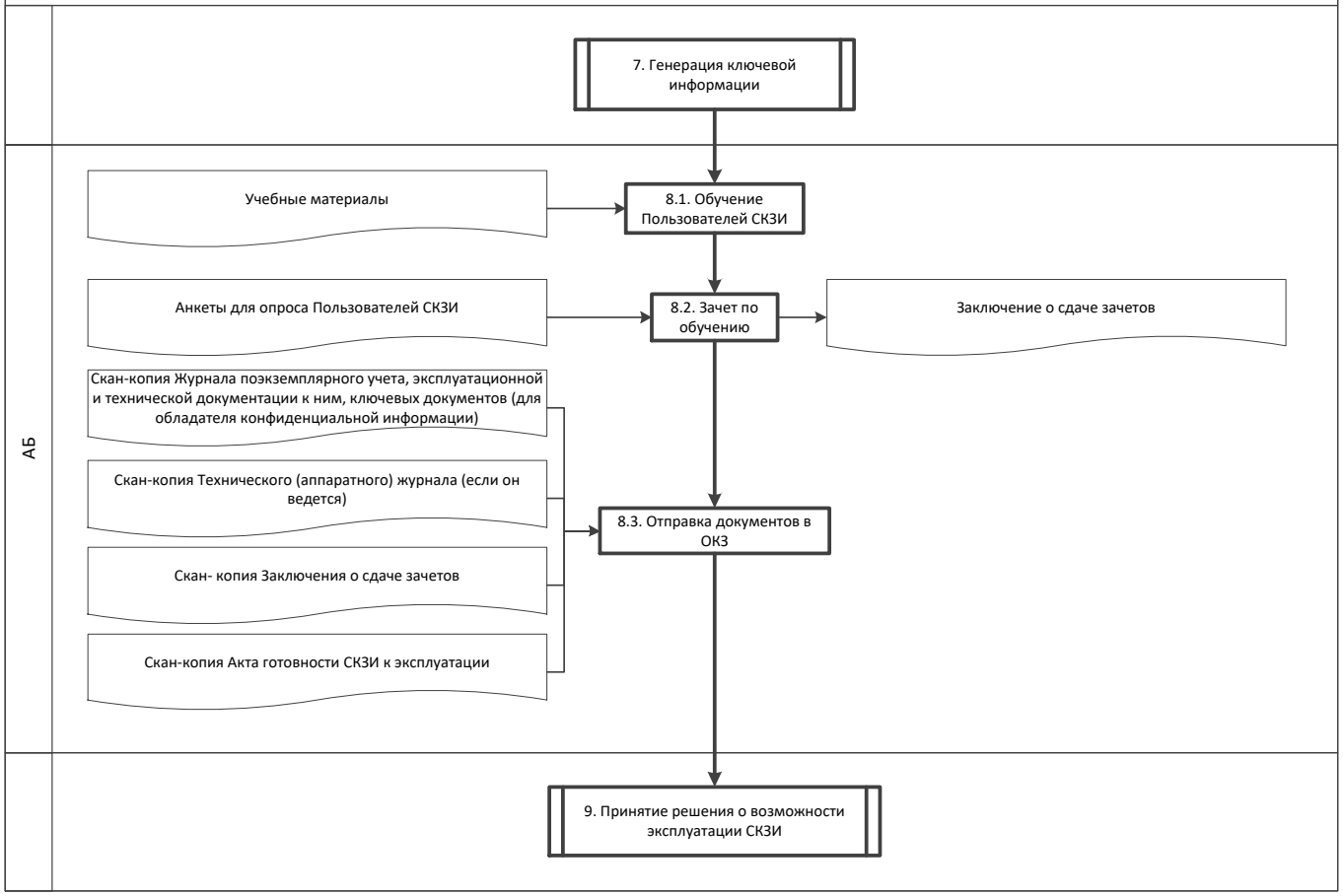
6. Подпроцесс «Установка и настройка СКЗИ»



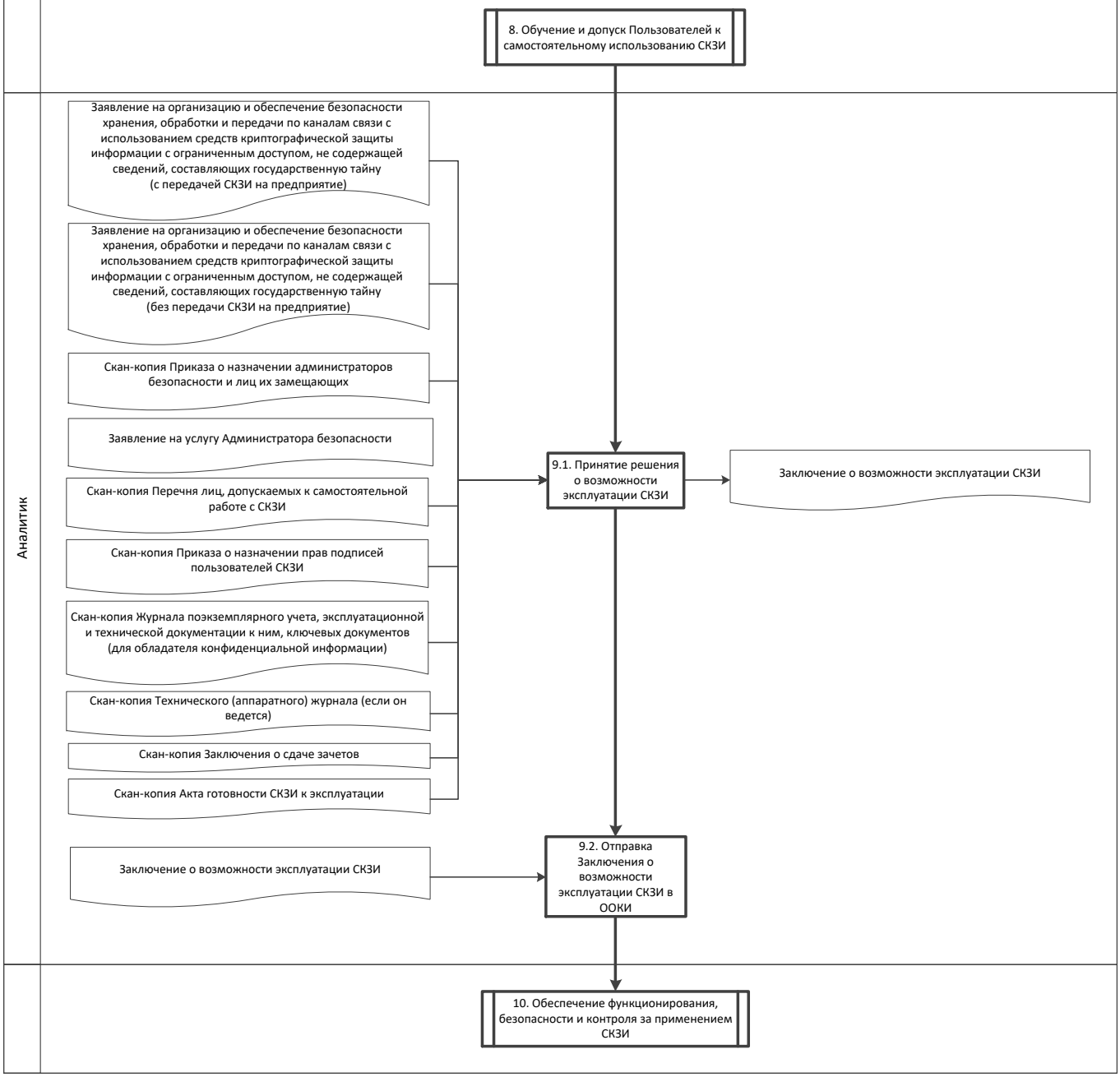
7. Подпроцесс «Генерация ключевой информации»



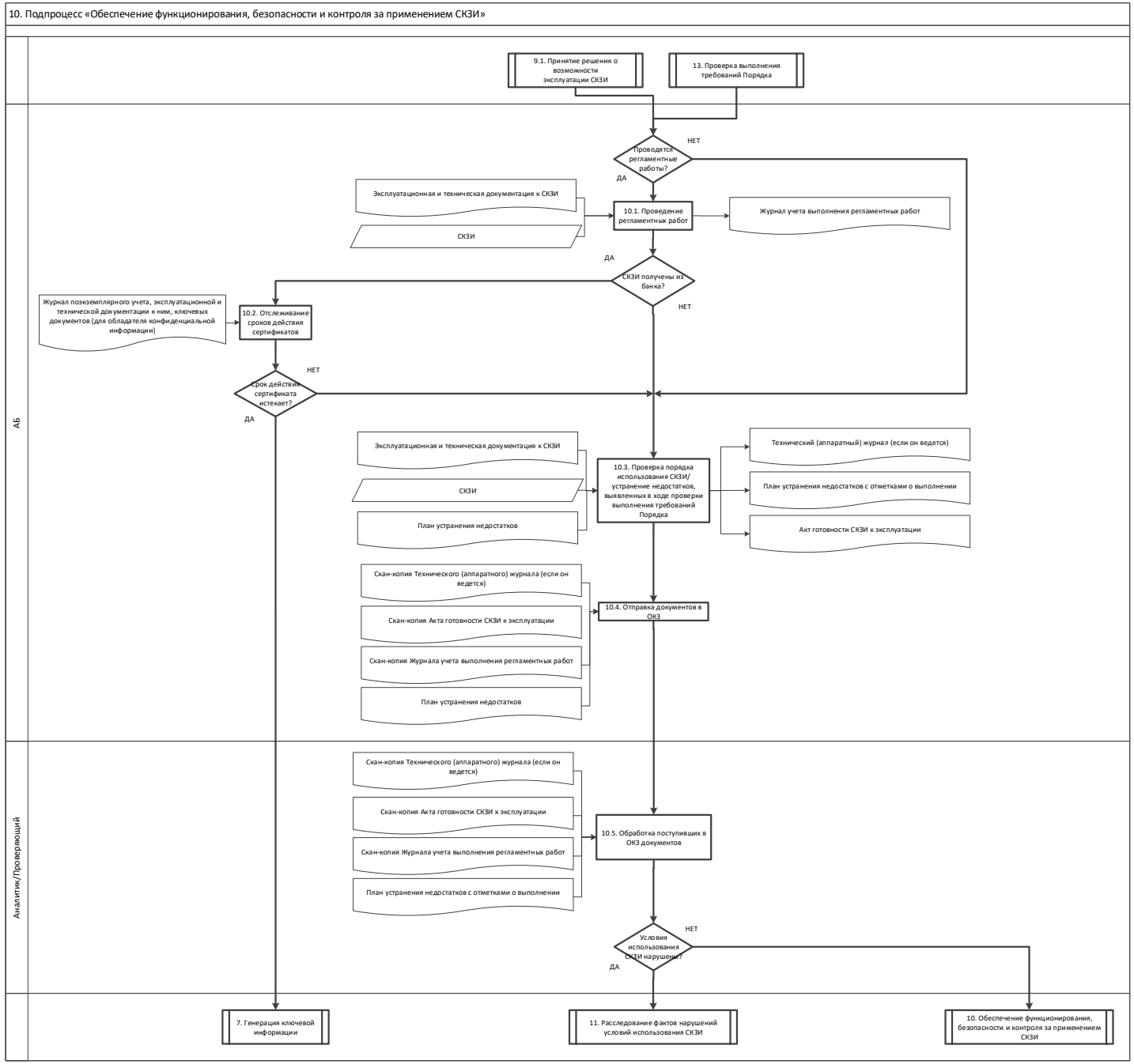
8. Подпроцесс «Обучение и допуск Пользователей к самостоятельному использованию СКЗИ»

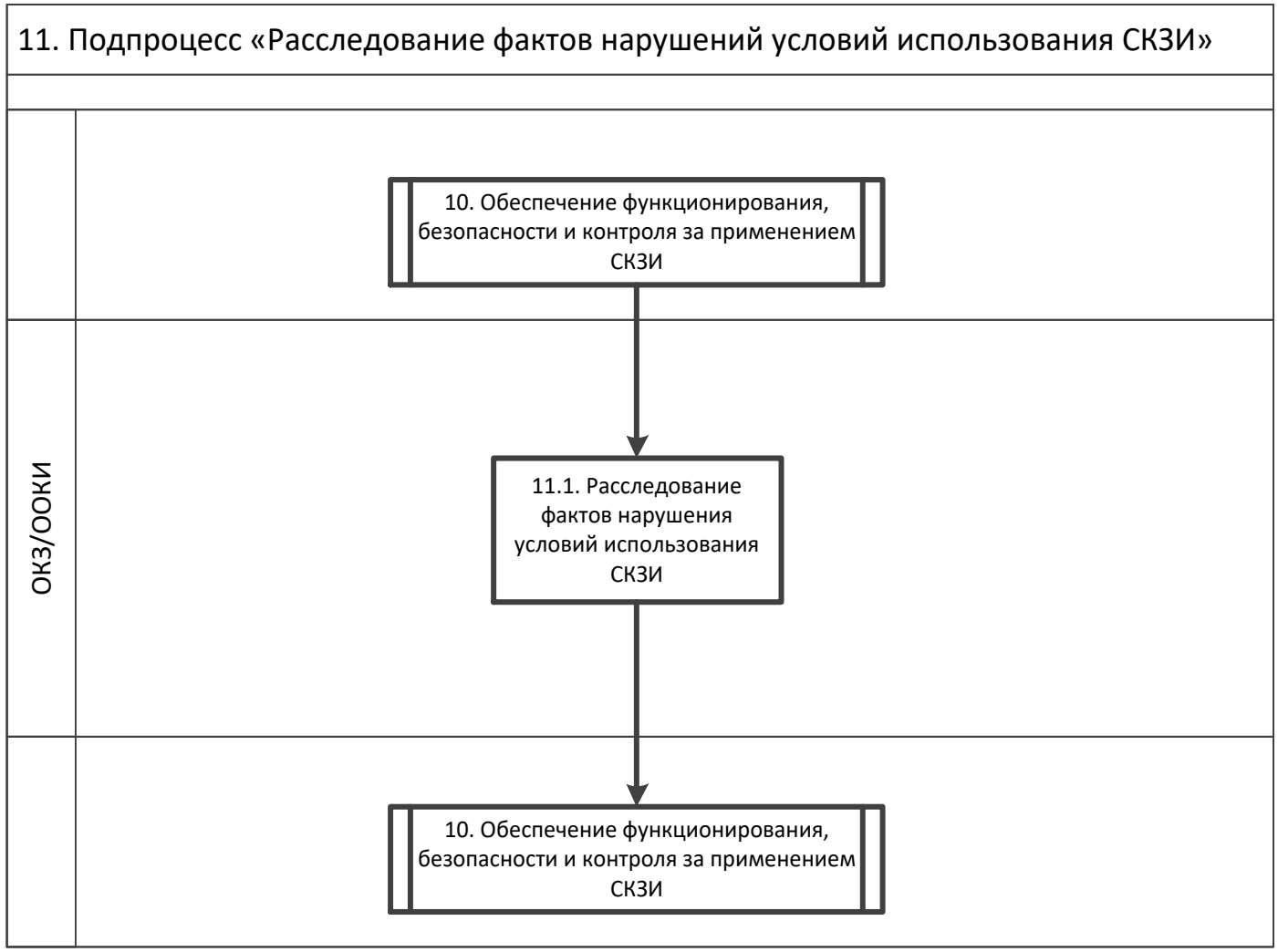


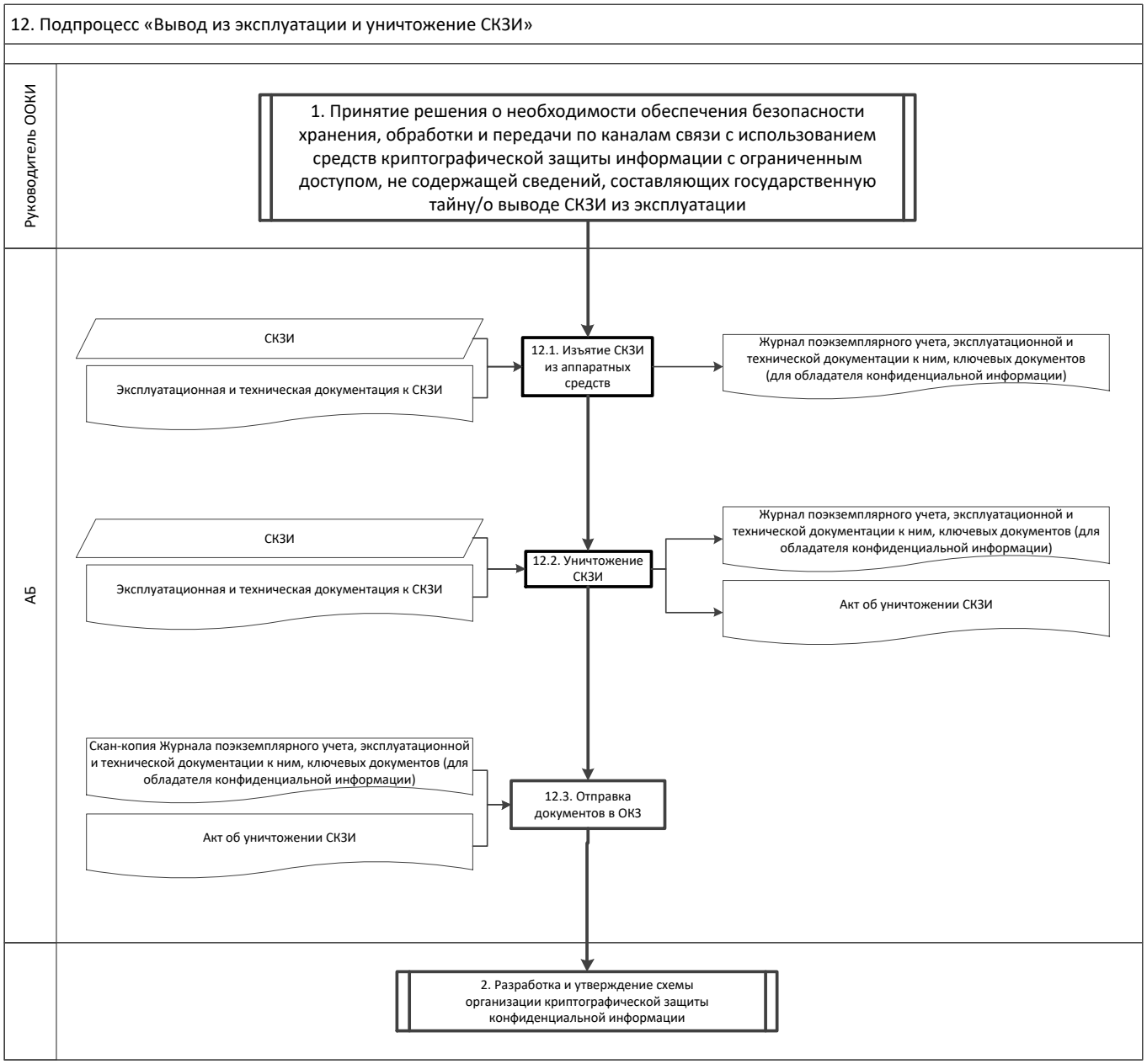
9. Подпроцесс «Принятие решения о возможности эксплуатации СКЗИ»



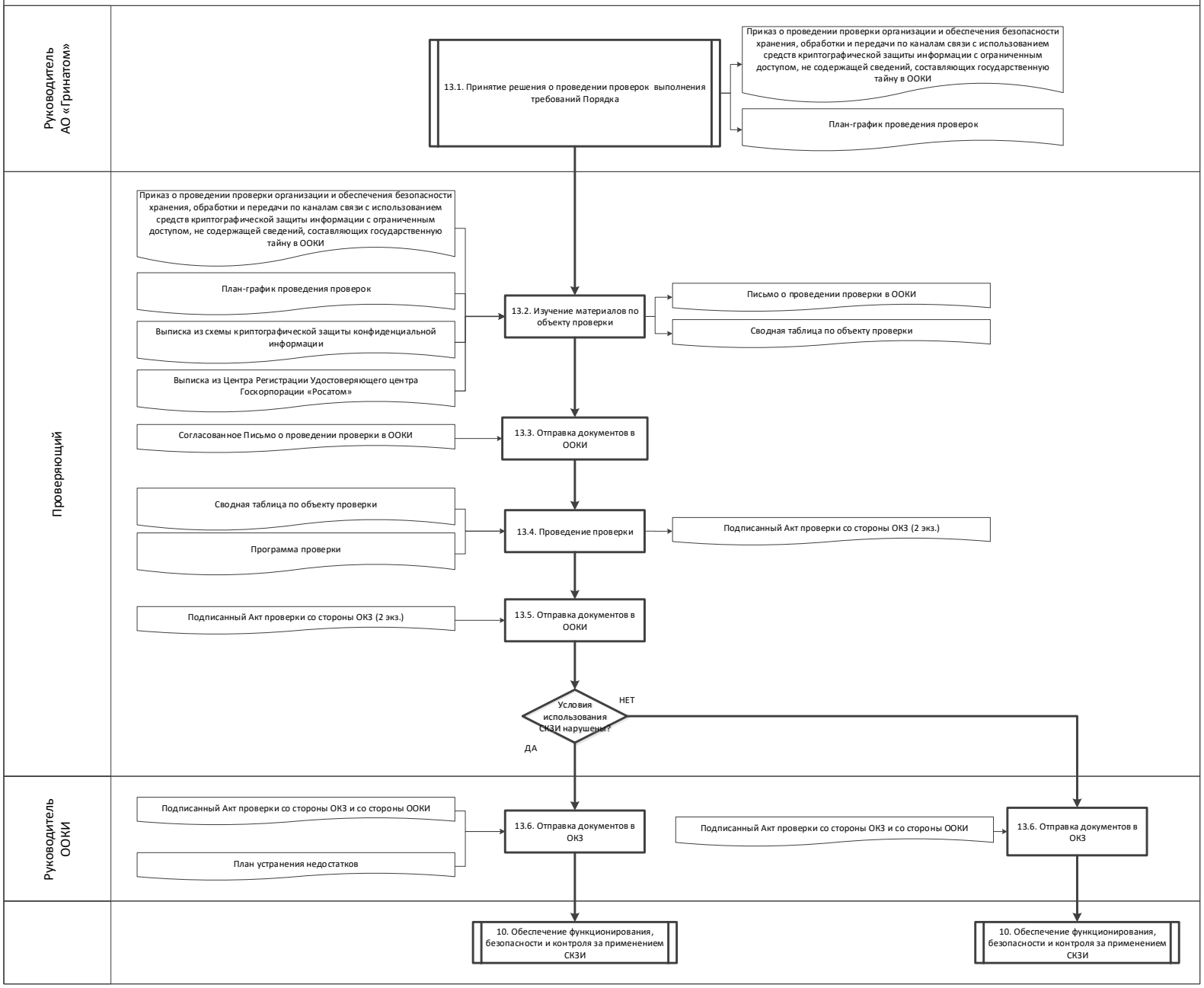
10. Подпроцесс «Обеспечение функционирования, безопасности и контроля за применением СКЗИ»




11. Подпроцесс «Расследование фактов нарушений условий использования СКЗИ»
ОКЗ/ООКИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ
11.1. Расследование фактов нарушения условий использования СКЗИ
10. Обеспечение функционирования, безопасности и контроля за применением СКЗИ


12. Подпроцесс «Вывод из эксплуатации и уничтожение СКЗИ»
Руководитель ООКИ
АБ
1. Принятие решения о необходимости обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну/о выводе СКЗИ из эксплуатации
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.1. Изъятие СКЗИ из аппаратных средств
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
СКЗИ
Эксплуатационная и техническая документация к СКЗИ
12.2. Уничтожение СКЗИ
Журнал поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
Скан-копия Журнала поэкземплярного учета, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)
Акт об уничтожении СКЗИ
12.3. Отправка документов в ОКЗ
2. Разработка и утверждение схемы организации криптографической защиты конфиденциальной информации

13. Подпроцесс «Проверка выполнения требований Порядка»



Приложение №3. Дополнительные выходы и дополнительные входы

№ п/п	Наименование дополнительного выхода процесса	Потребитель дополнительного выхода процесса (группа процессов/ внешний контрагент)

№ п/п	Наименование дополнительного входа процесса	Поставщик дополнительного входа процесса (группа процессов/ внешний контрагент)

Приложение №4. Форма приказа о назначении Администраторов безопасности и лиц их замещающих

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

« ___ » _____ 20 ___ г. № _____
(дата)

О назначении администраторов безопасности и лиц их замещающих

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. Назначить администраторами безопасности и возложить функции органа криптографической защиты по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, контроля за соблюдением требований безопасности, а также функции доверенного лица удостоверяющего центра по приему заявлений на выдачу сертификатов ключей проверки электронной подписи и по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра на следующих сотрудников:

   ФИО (полностью) _____
   Должность, подразделение _____
   Контактный телефон _____
   E-mail _____

   ФИО (полностью) _____
   Должность, подразделение _____
   Контактный телефон _____
   E-mail _____
2. Администраторам безопасности провести инструктаж и обучение Пользователей СКЗИ и ознакомить под расписку с правилами эксплуатации СКЗИ.
3. Контроль исполнения настоящего Приказа оставляю за собой.

_____ _____ _____
(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

Приложение №5. Форма Заявления на услугу Администратора безопасности

Заявление
на услугу Администратора безопасности

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ « _____ » _____ 20 _____ г.
(нужное подчеркнуть)

_____

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает предоставление услуги Администратора безопасности (код услуги GEN.23), для обслуживания защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем согласно перечню

№ п/п	Пользователь СКЗИ (должность, Ф.И.О.)	Установленное СКЗИ	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Адрес месторасположения АРМ

<УПОЛНОМОЧЕННОЕ ДОЛЖНОСТНОЕ ЛИЦО> _____/_____
(подпись) (ФИО)

М.П.

Приложение №5.1 Форма Заявления на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя

Заявление
на услугу по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ (нужное подчеркнуть) «_____» _____ 20 _____ г.

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает предоставление услуги по сопровождению учетной записи с электронной подписью в информационной системе, защищенной средствами криптографической защиты информации на АРМ пользователя (код услуги GEN.43), согласно перечню:

№ п/п	Владелец ключа (Ф.И.О., полностью)	Тип ключа	Сроки действия ключа	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Адрес месторасположения АРМ

Уполномоченное должностное лицо

_____ _____ _____
(подпись) (ФИО)

М.П.

Приложение №6. Перечень лиц, допускаемых к самостоятельной работе с СКЗИ

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«____» _____ 20 ___ г. № _____

(дата)

О назначении лиц, допускаемых к самостоятельной работе с СКЗИ

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. К работе с СКЗИ допустить следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность

2. Контроль исполнения настоящего Приказа оставляю за собой.

_____ _____ _____

(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

Приложение №7. Форма Приказа о предоставлении прав подписей в системе(ах)

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

«____» _____ 20 ___ г. № _____

(дата)

О предоставлении прав подписей в системе(ах) <НАИМЕНОВАНИЕ СИСТЕМЫ>

В соответствии с пунктами 7.5-7.6 Инструкции Банка России от 30.05.2014 №153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов» для осуществления платежей с использованием системы <НАИМЕНОВАНИЕ СИСТЕМЫ>

ПРИКАЗЫВАЮ:

1. Предоставить право первой подписи в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____

(Ф.И.О., должность)

_____

(Ф.И.О., должность)

2. Предоставить право второй подписи в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____

(Ф.И.О., должность)

_____

(Ф.И.О., должность)

3. Предоставить право запроса выписки в системе <НАИМЕНОВАНИЕ СИСТЕМЫ>:

_____

(Ф.И.О., должность)

_____

(Ф.И.О., должность)

2. Контроль исполнения настоящего Приказа оставляю за собой.

_____	_____	_____
(должность руководителя)	(подпись руководителя)	(Ф.И.О. руководителя)

Приложение №8.1 Заявление на СКЗИ (с передачей СКЗИ)

Заявление
на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
(с передачей СКЗИ)

« _____ » _____ 20 _____ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

просит ОКЗ АО «Гринатом» организовать и обеспечить безопасность хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в рамках услуг лицензируемой деятельности для следующих автоматизированных рабочих мест (АРМ), указанных в таблице, для чего, в соответствии с «ЕОМУ по информационной безопасности Госкорпорации «Росатом» и её организациях» №1/4-П-дсп от 09.01.2019 в организации, расположенной по адресу:

_____

функции ОКЗ возлагаются на администраторов безопасности, назначенных Приказом № _____ от _____ . Копия Приказа прилагается.

№ п/п	Пользователь СКЗИ (Ф.И.О. полностью)	Вид защищаемой информации	Автоматизированная/ информационная система	Тип СКЗИ	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение (предприятие)	Адрес месторасположения АРМ	Общесистемное программное обеспечение, установленное на АРМ
1								

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

М.П.

Приложение №8.2 Заявление на СКЗИ (без передачи СКЗИ)

Заявление
на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
(без передачи СКЗИ)

« _____ » _____ 20 _____ г.

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
фамилия, имя, отчество

действующего на основании _____

просит ОКЗ ЗАО «Гринатом» организовать и обеспечить безопасность хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в рамках услуг лицензируемой деятельности для следующих автоматизированных рабочих мест (АРМ), указанных в таблице, для чего, в соответствии с «ЕОМУ по информационной безопасности Госкорпорации «Росатом» и её организациях» №1/4-П-дсп от 09.01.2019 в организации, расположенной по адресу:

_____

функции ОКЗ возлагаются на администраторов безопасности, назначенных Приказом № _____ от _____ . Копия Приказа прилагается.

№ п/п	Пользователь СКЗИ (Ф.И.О. полностью)	Вид защищаемой информации	Наименование СКЗИ, версия	Номер лицензии, код лицензии, код конечного пользователя	Автоматизированная/ информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение	Адрес месторасположения АРМ	Общесистемное программное обеспечение, установленное на АРМ
1									

Администратор безопасности

_____/_____
(подпись) (ФИО)

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____/_____
(подпись) (ФИО)

м.п.

Приложение №9. Схема организации криптографической защиты конфиденциальной информации (шаблон)

			№ п/п
			Краткое наименования предприятия
			Полное наименование предприятия
			Заявление о присоединении №
			Администратор безопасности (ФИО, Приказ/
			Пользователь СКЗИ (ФИО полностью)
			Тип используемого СКЗИ
			Серийный номер СКЗИ
			Автоматизированная/информационная система
			Учетный/серийный номер системного блока АРМ, на котором установлено СКЗИ
			Системный блок АРМ опечатан печатью №
			Адрес местоположения АРМ
			Программное обеспечение, установленное на АРМ
			Вид защищаемой информации
			Рег. номер заключения о сдаче зачетов
			Дата регистрации заключения о сдаче зачетов
			Рег. номер акта готовности
			Дата регистрации акта готовности
			Рег. номер лицевого счета / ЖПУ
			Дата регистрации лицевого счета / ЖПУ
			Рег. номер Приказа о лицах допускаемых к самостоятельной работе с СКЗИ
			Дата регистрации Приказа о лицах, допускаемых к самостоятельной работе с
			Рег. номер Приказа о предоставлении прав подписей в платежных системах
			Дата регистрации Приказа о предоставлении прав подписей в
			Заключение о возможности эксплуатации СКЗИ
			Примечание

ГРИНАТОМ

Приложение №10. Книга лицевых счетов

Приложение 1 к Инструкции,
утвержденной приказом Федерального агентства
правительственной связи и информации
при Президенте Российской Федерации
от 13.05.2001 г. № 152

Книга лицевых счетов СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

Начат «___» _____ 201___ г.
Окончен «___» _____ 201___ г.
На ____ листах

Опись лицевых счетов

1			41		
2			42		
3			43		
4			44		
5			45		
6			46		
7			47		
8			48		
9			49		
10			50		
11			51		
12			52		
13			53		
14			54		
15			55		
16			56		
17			57		
18			58		
19			59		
20			60		
21			61		
22			62		
23			63		
24			64		
25			65		
26			66		
27			67		
28			68		
29			69		
30			70		
31			71		
32			72		
33			73		
34			74		
35			75		
36			76		
37			77		

- ЛИСТ -

№ пп	Фамилия Инициалы	№ по картотеке	Расписка лица оформившего л/с	Отметки о местонахождении

Лицевой счет _____ тел. _____

№ 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 рассылке (передаче)			Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении	Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Приложение №11. Доверенность доверенного лица на получение СКЗИ в ОКЗ

ДОВЕРЕННОСТЬ

доверенного лица, наделенного правом получения средств криптографической защиты информации

г. _____ «____»_____20__г.

_____

_____

(наименование организации, включая организационно-правовую форму)

в лице_____,

(должность)

действующего на основании_____

уполномачивает_____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

зарегистрированного по адресу: _____,

получать в Органе криптографической защиты АО «Гринатом» средства криптографической защиты информации.

Доверенное лицо наделяется правом подписи в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность действительна с момента выдачи по «___» _____ 20___г

Подпись доверенного лица _____ _____,

(фамилия, имя, отчество) (подпись)

подтверждаю.

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ДОЛЖНОСТНОГО ЛИЦА>

_____ _____ / _____

(подпись) (Ф.И.О.)

м.п.

Приложение №12. Сопроводительное письмо к СКЗИ

Акционерное общество «Гринатом»
(АО «Гринатом»)

1-й Нагатинский проезд, д. 10, стр. 1,
Москва, 115230
Телефон (499) 949-49-19, факс (499) 949-44-46
E-mail: info@greenatom.ru
ОКПО 64509942, ОГРН 1097746819720
ИНН 7706729736, КПП 770601001

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О передаче СКЗИ

Уважаемый(ая) <ИМЯ, ОТЧЕСТВО>!

В ответ на Ваше «Заявление о присоединении к Договору на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств» и «Заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» высылаем копии лицензий на право использования средств криптографической защиты информации.
Данный конверт необходимо передать в Орган криптографической защиты администратору безопасности.

Приложение: 1. Копии лицензий СКЗИ «КриптоПро CSP» – __ шт.

С уважением,

Начальник Отдела криптографической защиты — <И.О. ФАМИЛИЯ> (по дов.

Исполнитель

Приложение №13. Акт повреждения упаковки

АКТ №_____

г. Москва «___» _____ 201__ г.

Администратор безопасности _____
(ФИО)

составил настоящий акт в том, что полученная упаковка повреждена <УКАЗАТЬ СТЕПЕНЬ ПОВРЕЖДЕНИЯ>.

Вывод:

В выводе указывается возможность/невозможность дальнейшего использования ключевой информации/СКЗИ в зависимости от степени повреждения упаковки.

В случае образования свободного доступа к содержимому упаковки, использование ключевой информации/СКЗИ невозможно.

_____/_____
(подпись) (Ф.И.О)

Приложение №14. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Приложение 2 к Инструкции,
утвержденной приказом Федерального агентства
правительственной связи и информации
при Президенте Российской Федерации
от 13.05.2001 г. № 152

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

№ 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		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, произведших подключение (установку)	Дата подключения (установки) подписи лиц, произведших подлкючение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографиической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение №15. Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ

Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ

Москва 2020 г.

Оглавление

1. Общие положения

Настоящий документ описывает порядок разрешительного доступа эксплуатирующего персонала и пользователей к автоматизированным рабочим местам (АРМ) с установленными средствами криптографической защиты (СКЗИ).

2. Требования к размещению технических средств установленными СКЗИ

При размещении технических средств с установленными СКЗИ необходимо выполнять следующие требования:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования к программному и аппаратному обеспечению

Технические средства с установленными СКЗИ должны отвечать следующим требованиям:

- На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ. В случае технологических потребностей организации, эксплуатирующей СКЗИ, в использовании иного программного обеспечения, его применения должно быть санкционировано администратором безопасности. В любом случае ПО не должно содержать в себе возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других подпрограмм;
  - модифицировать память, выделенную для других подпрограмм;
  - передавать управление в область собственных данных и данных других подпрограмм;
  - несанкционированное модифицировать файлы, содержащие исполняемые кода при их хранении на жестком диске;

  - использовать недокументированные фирмами-разработчиками функции.
- На ПЭВМ одновременно может быть установлена только одна разрешенная ОС;
- В BIOC ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
- Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация);
- Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

4. Защита информации от НСД

При использовании СКЗИ необходимо принять следующие организационные меры:

- Предоставить права доступа к рабочим местам с установленным СКЗИ только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ;
- Запретить осуществление несанкционированного администратором безопасности копирования ключевых носителей;
- Запретить передачу передачу ключевых носителей лицам, к ним недопущенным;
- Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ;
- Запретить запись на ключевые носители посторонней информации;
- Запретить оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- Хранить ключевые носители в опечатываемых пеналах, которые в свою очередь должны хранить в запираемых и опечатываемых сейфах.

Пользователь несет персональную ответственность за хранение личных ключевых носителей;

- Сдать ключевые носители в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей;
- Немедленно уведомлять Удостоверяющий центр о фактах утраты или недостачи ключевых носителей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации;
- Запрещается разглашать содержимое носителей ключевой информации и передавать носители лицам к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п., иные средства отображения информации;
- Перед началом процесса установки ПО со встроенными модулями СКЗИ, либо автономных программных модулей СКЗИ должен осуществляться контроль целостности устанавливаемого ПО;
- При каждом запуске ПЭВМ с установленным СКЗИ должен осуществляться контроль целостности программного обеспечения, входящего в состав СКЗИ, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ;
- Администратор безопасности должен периодически (не реже 1 раза в год) менять пароль на вход в BIOS;
- В случае обнаружения «посторонних» (незарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена;
- Пользователь должен запускать только те приложения, которые разрешены администратором;
- Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:
    - Не использовать нестандартные, измененные или отладочные ОС;
    - Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
    - Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;
    - Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;
    - ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
    - Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - Системный реестр;
  - Файлы и каталоги;
  - Временные файлы;
  - Журналы системы;
  - Файлы подкачки;
  - Кэшируемая информация (пароли и т.п.);
  - Отладочная информация.

  Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.
- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- Необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;
- При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты;
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- Организовать и использовать комплекс антивирусной защиты;

- Исключить одновременную работу в ОС с работающим СКЗИ и загружаемой ключевой информацией нескольких пользователей.

Приложение №16. Технический (аппаратный) журнал

Технический (аппаратный) журнал

№ п.п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографческий номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	

Приложение №17. Акт готовности СКЗИ к эксплуатации

Акт готовности СКЗИ к эксплуатации №_____

г. _____ «____» _____ 20 ____ г.

Администратор безопасности _____ ,
(ФИО полностью., e-mail)

составил настоящий акт в том, что произведена проверка готовности АРМ обладателя конфиденциальной информации

_____
(Наименование организации, фактический адрес)

к эксплуатации СКЗИ на соответствие «ЕОМУ по информационной безопасности Госкорпорации «Росатом» и её организациях» №1/4-П-дсп от 09.01.2019 и требованиям «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 при Президенте РФ № 152 от 13.06.2001 г.

Произведена проверка выполнения «Порядка разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ» Приложение №15 к Порядку организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, операционная система настроена в соответствии с документацией на СКЗИ.

СКЗИ установлено:

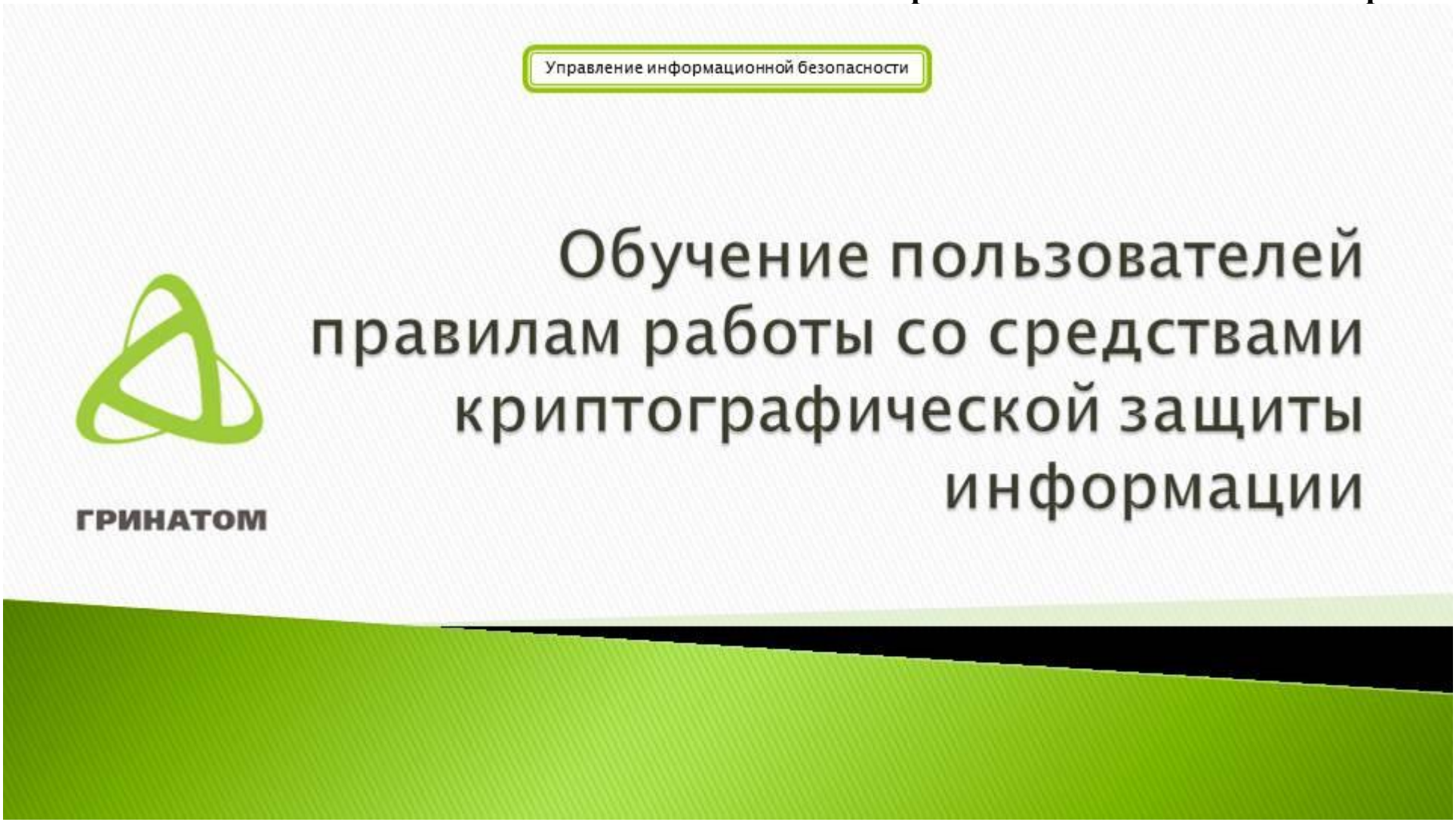
№ п/п	ФИО пользователя СКЗИ полностью	№ помещения и рабочего места	Уч.№ ПЭВМ	ПЭВМ опечатана печатью №	Наименование СКЗИ и версия	Версия ОС	Установлено сертифицированное	
							Антивирусное средство	СЗИ от НСД

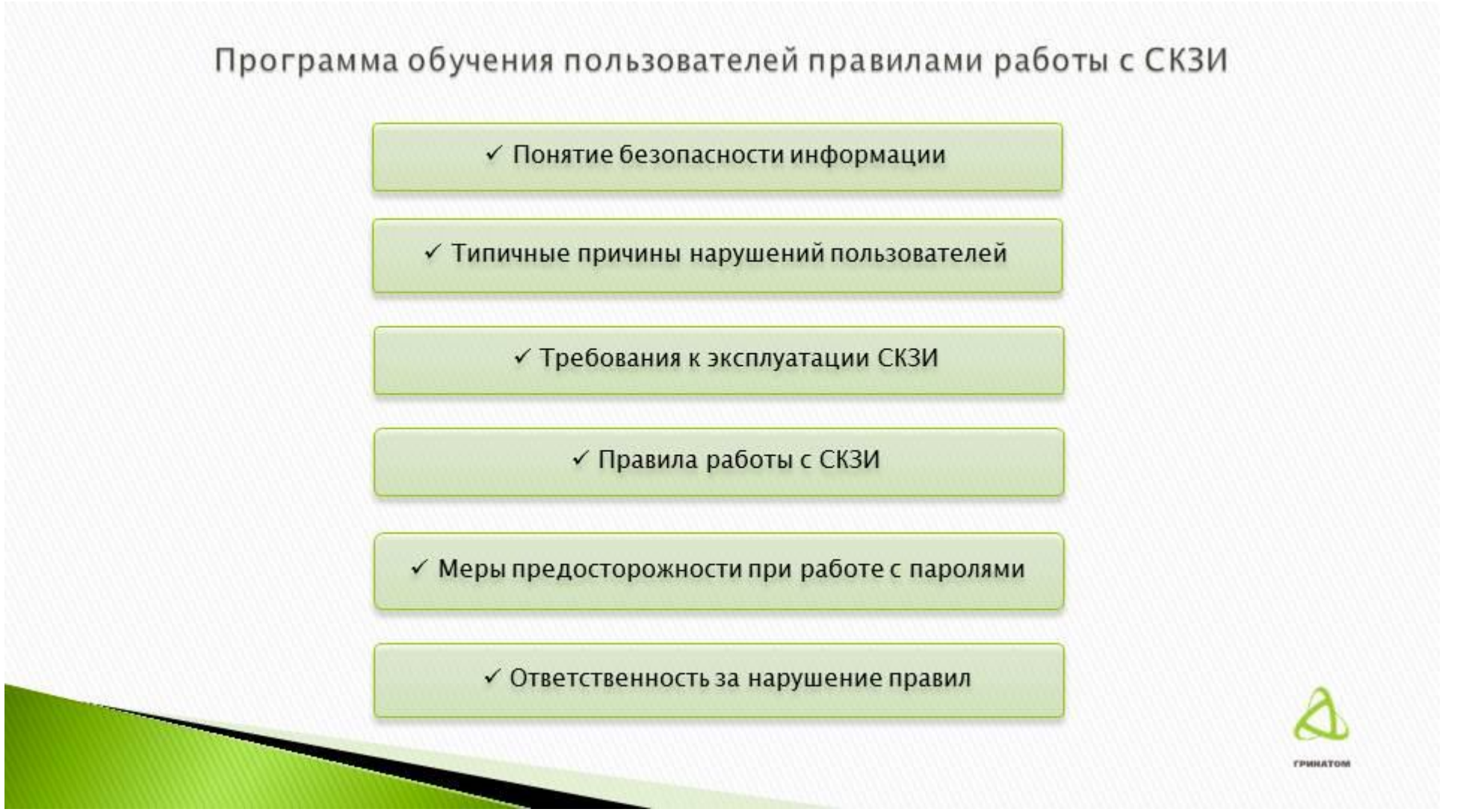
Вывод:

Оборудование АРМ соответствует Отраслевым требованиям по информационной безопасности №1/4-П-дсп от 09.01.2019 и требованиям «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 при Президенте РФ № 152 от 13.06.2001 г., их функционирование проверено и готово к эксплуатации с установленным СКЗИ.

_____ / _____
(подпись) (ФИО адм.безопасности)

Приложение №18. Учебные материалы




Программа обучения пользователей правилами работы с СКЗИ
✓ Понятие безопасности информации
✓ Типичные причины нарушений пользователей
✓ Требования к эксплуатации СКЗИ
✓ Правила работы с СКЗИ
✓ Меры предосторожности при работе с паролями
✓ Ответственность за нарушение правил
ГРИНАТОМ

Корпоративные ценности АО «Гринатом»

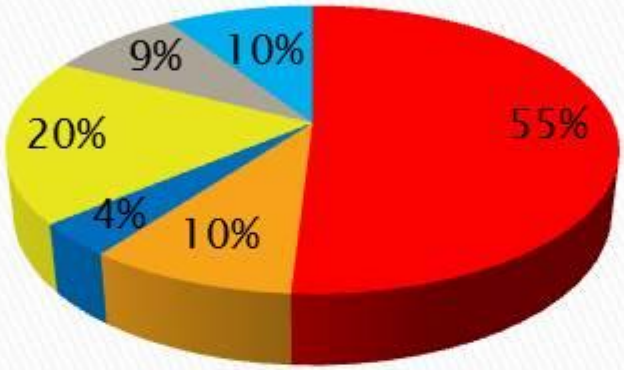
Корпоративные ценности компании - система принципов, на которых основывается ее деятельность, организация труда и стиль поведения сотрудников.
У компании «Гринатом» 6 ценностей:

- ✓ **Ответственность за результат**
- ✓ **Эффективность**
- ✓ **Уважение**
- ✓ **Безопасность**
- ✓ **Единая команда**
- ✓ **На шаг впереди**

Безопасность – наивысший приоритет. В нашей работе мы в первую очередь обеспечиваем полную безопасность людей и окружающей среды. В безопасности нет мелочей – мы знаем правила безопасности и выполняем их, пресекая нарушения. Особое внимание мы уделяем надежности/доступности сервисов и корпоративных информационных систем. Наши клиенты могут быть спокойны за сохранность их данных. Мы соблюдаем все внутренние регламенты и процедуры.

ГРИНАТОМ

Влияние осведомленности пользователей на уровень информационной безопасности



- Ошибки персонала
- Нечестные сотрудники
- Вирусы
- Проблемы электропитания
- Обиженные сотрудники
- Внешние нападения

Более 50 процентов от общего объема нарушений и преступлений составляют ошибки персонала

Обеспечение безопасности – задача всех работников организации

Пожарная безопасность обеспечивается не только пожарной дружиной, но и всеми сотрудниками, которые соблюдают установленные правила (не бросают окурки, не пользуются неисправленными электроприборами и т.п.).

Состояние безопасности предприятия (как информационной, так и пожарной) **зависит от каждого**

В состав системы обеспечения информационной безопасности входят все сотрудники, имеющие прямое или косвенное отношение к системе

ГРИНАТОМ

Типичные причины нарушений пользователей

- Использование ресурсов не по назначению

Действие:

использование предоставленных сотрудникам аппаратно-программных средств ГК «Росатом» в личных (иных, кроме служебных) целях

Последствия:

потери из-за непроизводительного использования ресурсов АС и рабочего времени, создание помех и дополнительных угроз основным технологическим процессам

Контрмеры:

запрет или введение существенных ограничений на использование аппаратно-программных средств не по назначению (в личных целях)

Пользователь не имеет право использовать предоставленные ему ресурсы ГК «Росатом» в личных целях

ГРИНАТОМ


Типичные причины нарушений пользователей
Непринятие мер по предотвращению порчи или утраты оборудования
Действие:
неумышленная порча или непринятие мер по предотвращению порчи или утраты (хищения) технических средств, носителей информации, повреждение линий связи...
Последствия:
прямой материальный ущерб. Частичный или полный отказ системы - потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технологических процессов)
Контрмеры:
повышение ответственности за сохранность и физическую целостность аппаратных средств (материальная компенсация в пользу ГК «Росатом»)
Если пользователь оказался свидетелем порчи имущества ГК «Росатом» он должен незамедлительно сообщить о произошедшем непосредственному руководителю
ГРИНАТОМ

Типичные причины нарушений пользователей

- Несанкционированное изменение конфигурации устройств и программ

Действие:

самовольное изменение состава и конфигурации используемых аппаратных и программных средств, отключение или изменение режимов работы оборудования и программ

Последствия:

частичный или полный отказ системы.
Потери из-за простоев и затраты на восстановление ресурсов и работоспособности (технологических процессов), внедрение «жучков»

Контрмеры:

введение запретов и повышение ответственности за физическую целостность аппаратно-программных ресурсов

Пользователю запрещается: вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры, добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности, инсталляция сторонних программ, внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

ГРИНАТОМ

Типичные причины нарушений пользователей

- Инсталляция и/или запуск сторонних программ на рабочих станциях

Действие:

несанкционированное внедрение и использование неразрешенных и сторонних программ, не имеющих отношения к производственной деятельности

Последствия:

необоснованный расход ресурсов системы (загрузка процессора, каналов связи, оперативной памяти и памяти на внешних носителях), возникновение конфликтов ПО, заражение компьютеров вирусами

Контрмеры:

запрет самостоятельной разработки, установки и использования неучтенных, не разрешенных программ (не относящихся к производственному процессу)

ГРИНАТОМ

Типичные причины нарушений пользователей

- Отключение или создание помех для работы штатных антивирусных программ

Действие:

отключение или создание препятствий для работы антивирусных программ, неправильные действия в случае обнаружения вирусов

Последствия:

потери из-за заражения компьютера вирусами и распространение эпидемии на другие сервера и рабочие станции (потеря данных, компрометация конфиденциальных сведений, простои системы, затраты на восстановление)

Контрмеры:

повышение ответственности пользователей, внедрение более совершенных антивирусных средств

При обнаружении вирусного заражения ЭВМ пользователь обязан прекратить обработку информации на компьютере и сообщить о произошедшем в подразделение информационной безопасности, эксплуатирующей систему

ГРИНАТОМ

Типичные причины нарушений пользователей

- Использование нелицензионного программного обеспечения

Действие:

использование нелицензионного программного обеспечения на компьютерах предприятий отрасли (пиратских копий программ)

Последствия:

судебные иски правообладателей на компенсацию ущерба, возбуждение уголовного дела по ст. 146 УК РФ «Нарушение авторских и смежных прав» и связанные с этим риски, потеря репутации, выход из строя ряда АС

Контрмеры:

повышение ответственности конечных пользователей и обслуживающего персонала, усиление контроля, применение средств создания замкнутой программной среды

ГРИНАТОМ

Типичные причины нарушений пользователей

- Нарушение порядка формирования, использования, хранения и резервного копирования критичной информации

Действие:

непреднамеренное удаление или искажение программ и файлов с важной (не обязательно конфиденциальной) информацией, ввод ошибочных данных и т.п.

Последствия:

потери из-за простоев и затраты на восстановление ресурсов и работоспособности

Контрмеры:

упорядочение работы (наведение порядка), повышение ответственности исполнителей, внедрение процедур резервного копирования важных данных

ГРИНАТОМ

Типичные причины нарушений пользователей

- Самовольное создание и использование разделяемых сетевых ресурсов

Действие:

самовольное создание совместно используемых сетевых ресурсов (папок общего пользования) на своих компьютерах, несанкционированное удаление или изменение прав доступа к ним

Последствия:

создание дополнительных угроз вирусного проникновения и НСД, связанных с потерей данных или компрометацией конфиденциальных сведений, затруднение резервного копирования и контроля обмена данными

Контрмеры:

повышение ответственности пользователей, использование настроек ОС (отключение служб, настройка сетевых фильтров и т.п.)

ГРИНАТОМ

Типичные причины нарушений пользователей

- Личная (непроизводственная) переписка по электронной почте

Действие:

злоупотребления при осуществлении личной переписки по электронной почте, претензии сотрудников на тайну личной переписки

Последствия:

непроизводительная трата ресурсов и рабочего времени (снижение продуктивности работы сотрудников), создание помех технологическим процессам, внутренние конфликты, подрыв репутации ГК «Росатом»

Контрмеры:

повышение ответственности сотрудников, подписание соглашений о контроле за перепиской

ГРИНАТОМ


Типичные причины нарушений пользователей
Пересылка конфиденциальных сведений ГК «Росатом» в открытом виде
Действие:
пересылка конфиденциальной корпоративной информации в открытом виде, отправка писем посторонним лицам по ошибочным адресам, использование дополнительных личных почтовых ящиков на внешних (сторонних) почтовых серверах и т.п.
Последствия:
утечка конфиденциальной информации (в том числе коммерческих секретов)
Контрмеры:
повышение ответственности, применение Защищенной корпоративной почтовой системы
Пересылка конфиденциальных сведений ГК «Росатом» осуществляется установленным порядком с помощью защищенных с использованием шифровальных (криптографических) средств систем
ГРИНАТОМ

Типичные причины нарушений пользователей

- Использование доступа в Интернет в непроизводственных целях
- Посещение хакерских или взломанных хакерами сайтов

Действие:

посещение сторонних сайтов (информационных, развлекательных, электронных магазинов или каталогов и т.п.), загрузка различных файлов, посещение хакерских или взломанных хакерами (зараженных) и других подозрительных сайтов (содержащих повушки и вредоносные коды)

Последствия:

непроизводительные затраты ресурсов, создание помех основным технологическим процессам, вирусное заражение, загрузка троянских и других вредоносных программ, возможность обвинения во взломе данных сайтов, непреднамеренная пересылка конфиденциальной информации («фишинг»)

Контрмеры:

повышение ответственности пользователей, установка средств фильтрации трафика по адресам сайтов, безопасная настройка Web-клиентов

ГРИНАТОМ

Приказ от 30.12.2019 №1/1517-П

4. Права и обязанности пользователя

п. 4.1. Пользователь имеет право заявлять потребность на подключение к ИТ-ресурсу, необходимому ему для исполнения своих обязанностей.

п.4.3.2 Использовать средства вычислительной техники автоматизированной системы организации, предоставляемые ИТ-ресурсы только в целях исполнения своих обязанностей.

4.3.3 Принимать меры по предотвращению использования ИТ-ресурсов другими лицами от его имени, обеспечивать сохранность и конфиденциальность паролей, кодов доступа и иной ключевой информации, используемой для авторизованного доступа к ИТ-ресурсам.

ГРИНАТОМ


Типичные причины нарушений пользователей
Нарушение правил использования средств криптографической защиты информации
Действие:
нарушение правил применения средств криптографической защиты информации
Последствия:
утрата криптографических ключей, требующая их замены в системе (выход из строя ключевого носителя). Компрометация секретных ключей, используемых для шифрования и ЭП файлов и защиты удаленного взаимодействия. Злоумышленник может получить доступ к зашифрованной конфиденциальной информации, доступ в корпоративную сеть с правами пользователя скомпрометированного ключа, а также в случае компрометации секретного ключа ЭП может подделывать подписи его владельца
Контрмеры:
обучение пользователей правилам работы со средствами криптографической защиты информации (СКЗИ), сдача зачетов по программе обучения
К самостоятельной работе к СКЗИ допускаются пользователи сдавшие зачеты по программе обучения правилам работы с СКЗИ. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты (ОКЗ). Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего ОКЗ на основании принятых от этих лиц зачетов по программе обучения.
ГРИНАТОМ

Требования к эксплуатации СКЗИ

- Средствами СКЗИ НЕ ДОПУСКАЕТСЯ обрабатывать информацию, содержащую сведения, составляющие государственную тайну;
- Ключевая информация является конфиденциальной;
- Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП (определяется при сертификации СКЗИ);
- СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах;
- Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

ГРИНАТОМ

Требование к размещению технических средств с установленными СКЗИ

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленными СКЗИ, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе

ГРИНАТОМ

Требования к программному и аппаратному обеспечению

- На технических средствах, оснащенных СКЗИ должно использоваться только лицензионное программное обеспечение фирм-производителей, либо ПО, сертифицированное ФСБ. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование СКЗИ;
- На ПЭВМ одновременно может быть установлена только одна разрешенная ОС;
- В BIOC ПЭВМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС;
- Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация);
- Запрещается подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

ГРИНАТОМ

Правила использования и хранения ключевых носителей

ЗАПРЕЩАЕТСЯ:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации; при уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- вносить какие-либо изменения в программное обеспечение СКЗИ; в случае исчезновения на компьютере системы использующей средства криптографической защиты – сообщить в службу информационной безопасности и прекратить работу с любой доступной на компьютере системой до выявления причины;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- разглашать пароль другим лицам;
- записывать на ключевые носители постороннюю информацию;

Федеральный закон от 06.04.2011 №63 ФЗ «Об электронной подписи»

ст.10 п.1 При использовании усиленных электронных подписей участники электронного взаимодействия обязаны: обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия

ГРИНАТОМ

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Ключевые носители должны храниться в опечатываемых пеналах, которые в свою очередь необходимо помещать в опечатываемые сейфы. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

ГРИНАТОМ

Приказ от 09 февраля 2005 г. № 66

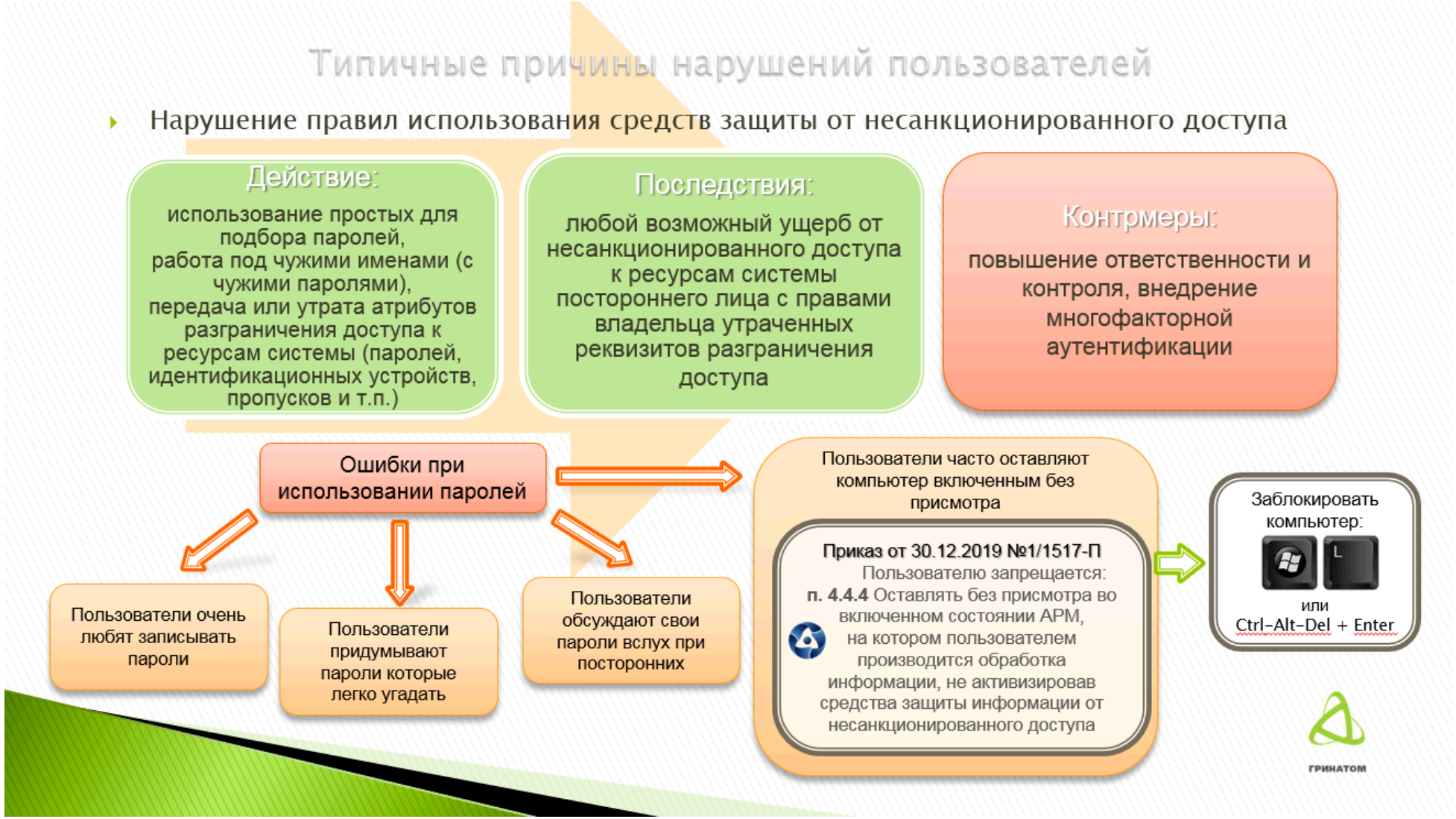
пп. 46 СКЗИ эксплуатируются в соответствии с правилами пользования ими...

пп. 51 Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

- обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
- собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
- ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

ГРИНАТОМ

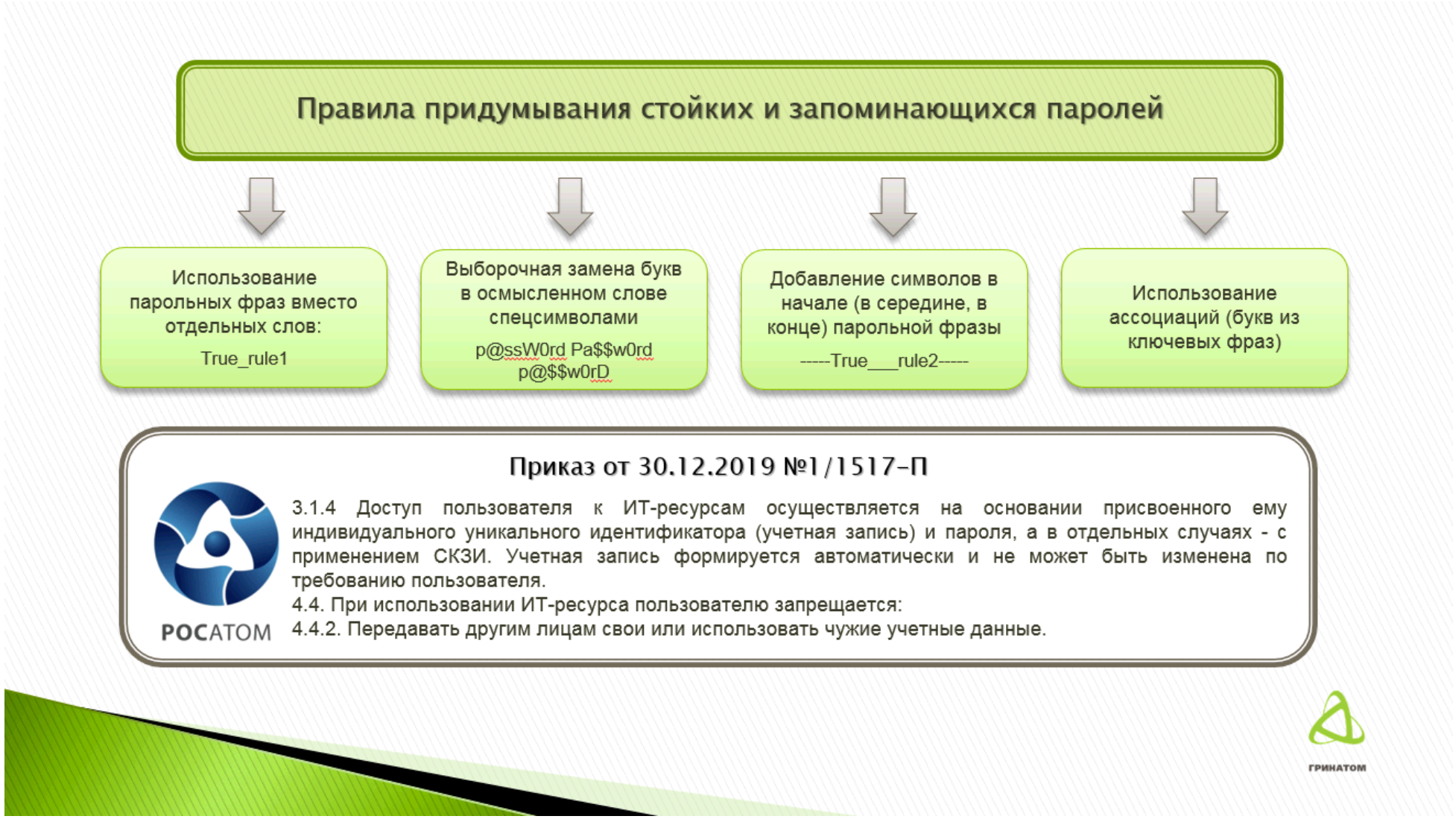

Компрометация ключей
утрата ключевого носителя с последующим обнаружением
увольнение сотрудников, имевших доступ к ключевой информации
нарушение печатей на сейфе с ключевыми носителями
временное оставление ключевого носителя без присмотра
случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями
нарушение печатей пеналов, в которых хранятся ключевые носители
Компрометация – это любая возможность (или совершившийся факт) попадания ключей посторонним (не допущенным) лицам. В случае утери действующего ключевого носителя с ЭП, а также обнаружения после потери – немедленно направить администратору безопасности сообщение о компрометации ключей ЭП
ГРИНАТОМ


Типичные причины нарушений пользователей
Нарушение правил использования средств защиты от несанкционированного доступа
Действие:
использование простых для подбора паролей,
работа под чужими именами (с чужими паролями),
передача или утрата атрибутов разграничения доступа к ресурсам системы (паролей, идентификационных устройств, пропусков и т.п.)
Последствия:
любой возможный ущерб от несанкционированного доступа к ресурсам системы постороннего лица с правами владельца утраченных реквизитов разграничения доступа
Контрмеры:
повышение ответственности и контроля, внедрение многофакторной аутентификации
Ошибки при использовании паролей
Пользователи очень любят записывать пароли
Пользователи придумывают пароли которые легко угадать
Пользователи обсуждают свои пароли вслух при посторонних
Пользователи часто оставляют компьютер включенным без присмотра
Приказ от 30.12.2019 №1/1517-П
Пользователю запрещается:
п. 4.4.4 Оставлять без присмотра во включенном состоянии АРМ, на котором пользователем производится обработка информации, не активизировав средства защиты информации от несанкционированного доступа
Заблокировать компьютер:
L
или
Ctrl-Alt-Del + Enter
ГРИНАТОМ

Меры предосторожности при работе с паролями

- Позаботьтесь, чтобы при вводе пароля за Вами не подглядывали (в том числе и с помощью камер видеонаблюдения);
- Когда вам оказывают техническую поддержку, всегда вводите свой пароль сами и никогда не выдавайте его;
- Не вводите свой пароль на чужих компьютерах;
- Не используйте один и тот же пароль для доступа к внутренним ресурсам ГК «Росатом» и для доступа к службам в сети Интернет;
- Периодически меняйте свой пароль. Следуйте правилам придумывания стойких и запоминающихся паролей;
- Если необходимо записать пароль, храните его в физически наиболее безопасном месте (в личном сейфе), либо используйте утвержденные ИБ программно-аппаратные средства;
- Если Вас кто-либо под каким-либо предлогом попросит сообщить Ваш пароль (социальный инжиниринг, «фишинг»), не поддавайтесь на уловку и незамедлительно доложите об этом Администратору безопасности.

ГРИНАТОМ


Правила придумывания стойких и запоминающихся паролей
Использование парольных фраз вместо отдельных слов:
True_rule1
Выборочная замена букв в осмысленном слове спецсимволами
p@ssW0rd Pa$$w0rd p@$$w0rD
Добавление символов в начале (в середине, в конце) парольной фразы
-----True___rule2-----
Использование ассоциаций (букв из ключевых фраз)
Приказ от 30.12.2019 №1/1517-П
3.1.4 Доступ пользователя к ИТ-ресурсам осуществляется на основании присвоенного ему индивидуального уникального идентификатора (учетная запись) и пароля, а в отдельных случаях - с применением СКЗИ. Учетная запись формируется автоматически и не может быть изменена по требованию пользователя.
4.4. При использовании ИТ-ресурса пользователю запрещается:
4.4.2. Передавать другим лицам свои или использовать чужие учетные данные.
РОСАТОМ
ГРИНАТОМ


Ответственность пользователя СКЗИ за разглашение конфиденциальной информации
Трудовой кодекс РФ
Кодекс РФ об административных правонарушениях
Уголовный кодекс РФ
ст.81 ТК РФ
Расторжение трудового договора по инициативе работодателя
ст.13.14 КОАП РФ
Наложение адм. штрафа от 500 до 1000 руб. (на граждан) и от 4000 до 5000 руб. (на должностных лиц)
ст.183 п.2 УК РФ
Наказывается штрафом в размере до 1 млн. руб. или лишением свободы сроком до трех лет


Ответственность организации
Кодекс РФ об административных правонарушениях
Уголовный кодекс РФ
ст.13.11-13.14 КОАП РФ
Штраф до 25 000 руб. с конфискацией, приостановление деятельности организации на срок до 90 суток
ст.137, 138, 171, 183, 272, 273, 274, 293 УК РФ
Наказание до 7 лет лишения свободы штраф до 1 млн. руб.

Самая большая ошибка - игнорирование установленных ограничений и правил политики безопасности при работе системы

Будьте внимательны и осторожны!

Помните об угрозах ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ!

Приложение №19. Анкета для опроса пользователей

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ
(для корректного заполнения просьба отметить один или несколько вариантов ответа)

1. Сколько процентов из общего объема нарушений и преступлений составляют ошибки персонала?
    a) 4%;
    b) 19%;
    c) 20%;
    d) >50%.

2. Кто входит в состав системы обеспечения информационной безопасности?
    a) сотрудники подразделения информационной безопасности;
    b) сотрудники Казначейства;
    c) все сотрудники ГК Росатом, имеющие прямое или косвенное отношение к системе.

3. Имеет ли право пользователь использовать предоставленные ему ресурсы ГК Росатом в личных целях?
    a) да;
    b) нет;
    c) иногда.

4. Что должен сделать пользователь, если он оказался свидетелем порчи имущества ГК Росатом?
    a) попытаться исправить испорченное имущество;
    b) попытаться предотвратить порчу имущества;
    c) незамедлительно сообщить непосредственному руководителю о произошедшем;
    d) не придавать этому значения.

5. Какие операции не имеет право производить пользователь с аппаратно-программными средствами, выданными ему ГК Росатом для исполнения своих служебных обязанностей?
    a) вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры;
    b) добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности ЭВМ;
    c) исполнение своих служебных обязанностей;

d) инсталляция сторонних программ на ЭВМ;
e) внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

6. Что должен сделать пользователь при обнаружении вирусного заражения ЭВМ?
    a) обновить базы антивируса, произвести проверку компьютера и удалить вирус;
    b) прекратить обработку информации на компьютере;
    c) сообщить в подразделение информационной безопасности, эксплуатирующей систему;
    d) перезагрузить компьютер;
    e) выключить компьютер и отсоединить от сети.

7. Что должен сделать пользователь при временном уходе с рабочего места?
    a) убрать в недоступное место записанные на бумаге пароли;
    b) завершить работу всех открытых приложений;
    c) заблокировать экран нажатием клавиш Ctrl-Alt-Del + Enter;
    d) выключить компьютер;
    e) ключевой носитель убрать в запираемое и опечатываемое хранилище.

8. Какие пользователи допускаются к самостоятельной работе с СКЗИ?
    a) все пользователи ГК Росатом;
    b) нуждающиеся в СКЗИ для исполнения своих служебных обязанностей;
    c) прошедшие обучение правилам работы с СКЗИ;
    d) сдавшие зачеты по программе обучения правилам работы с СКЗИ.

9. Какие обстоятельства относятся к компрометации ключей?
    a) утеря ключевого носителя с последующим обнаружением;
    b) утеря ключевого носителя;
    c) временное оставление ключевого носителя без присмотра;
    d) нарушение печатей на сейфе с ключевыми носителями;
    e) утеря ключей от сейфа, в котором хранятся ключевые носители.

10. Как должен действовать пользователь СКЗИ при утере ключевого носителя с последующим обнаружением, в случае когда нельзя достоверно установить, что произошло с ключевым носителем?
    a) незамедлительно поставить в известность о факте компрометации ключей администратора безопасности;
    b) самостоятельно произвести генерацию новых ключей ЭП, поставив в известность банк о факте компрометации;
    c) продолжить работу с найденными ключами.

11. Как обеспечить стойкий и легко запоминающийся пароль?

a) использовать парольные фразы;
b) придумать длинный пароль, но не менее 8-и символов;
c) выборочно заменить буквы спецсимволами;
d) добавить спецсимволы в начале (в середине, в конце);
e) использовать ассоциации;
f) использовать личные данные (ФИО, кличка собаки, марку машины, название улицы и пр.).

12. Какая ответственность предусмотрена законодательством РФ за нарушения правил работы с конфиденциальной информацией?
a) уголовная;
b) административная;
c) ответственность не предусмотрена.

13. Какая ответственность предусмотрена Уголовным кодексом РФ пользователю за разглашение коммерческой тайны?
a) штраф в размере до 1 млн. руб;
b) штраф в размере до 80 000 руб;
c) лишение свободы до двух лет;
d) лишение свободы до трех лет.

14. Ключевые носители ("флешки", "таблетки" и т.п.), содержащие действующие ключи ЭП, используемые для подписания платежных документов разрешается:
a) передавать работникам других департаментов;
b) передавать сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Ключевые носители, содержащие действующие ключи ЭП, запрещается передавать другим лицам.

15. Допускается сообщать пароль для доступа к ключевым носителям, содержащим действующие ключи ЭП, и используемым для подписания документов:
a) работникам других департаментов;
b) сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Пароль запрещается разглашать другим лицам.

16. В случае потери ключевого носителя, содержащего действующие ключи ЭП:

a) сообщить сотрудникам Госкорпорации для генерации новых ключей ЭП;
b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
c) направить администратору безопасности сообщение о компрометации ключей ЭП.

17. В случае обнаружения после потери своего ключевого носителя, содержащего действующие ключи ЭП:
a) сообщить сотрудникам Госкорпорации для генерации новых ключей ЭП;
b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
c) продолжить использование данного ключевого носителя без генерации новых ключей ЭП;
d) направить администратору безопасности сообщение о компрометации ключей ЭП.

18. Свой ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается временно передавать для работы:
a) сотрудникам Госкорпорации;
b) сотрудникам службы технической поддержки;
c) администратору безопасности;
d) только своему коллеге по подразделению;
e) ничего из вышеперечисленного. Ключевой носитель, содержащий действующие ключи ЭП, нельзя передавать другим лицам к ним не допущенным.

19. На ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается записывать файлы:
a) если они содержат служебные документы по профилю работы;
b) если есть свободное место на ключевом носителе и они содержат служебные документы по профилю работы;
c) нельзя записывать, даже если они содержат служебные документы по профилю работы.

20. Каким образом осуществляется пересылка конфиденциальных сведений ГК Росатом?
a) в открытом виде с использованием личных почтовых ящиков, зарегистрированных на внешних (сторонних) серверах;
b) с помощью защищенных с использованием шифровальных (криптографических) средств систем;
c) возможны оба варианта.

21. Какие требования предъявляются к хранению ключевых носителей, содержащих электронную подпись?
    a) ключевые носители хранятся в спецпомещениях, убранными в опечатанные хранилища;
    b) ключевые носители хранятся в спецпомещении, в ящике рабочего стола, закрытыми на ключ;
    c) ключевые носители хранятся в спецпомещении на рабочем столе пользователя;
    d) ключевые носители хранятся на связке обычных ключей.

22. Какие виды ответственности предусмотрены законодательством РФ для лиц, виновных в нарушении требований по защите конфиденциальной информации?
    a) ответственность не предусмотрена;
    b) дисциплинарная: расторжение трудового договора по инициативе работодателя;
    c) уголовная: 7 лет лишения свободы, штраф до 1 млн. руб;
    d) уголовная: штраф 500 000 руб;
    e) административная: штраф 30 000 руб, приостановление деятельности организации на срок до 90 суток.

Пользователь СКЗИ _____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

Зачтено/не зачтено

Проверил

Администратор безопасности

_____/_____
(подпись) (Ф.И.О)

«___» _____ 201__ г.

Приложение №20. Заключение о сдаче зачетов

Заключение о сдаче зачетов

№ п/п	Наименование организации	ФИО обучающегося	Зачтено/не зачтено

Состав проверяющей комиссии:

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_________________/__________________
(подпись) (Ф.И.О)

«___» _____________ 201__ г.

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_________________/__________________
(подпись) (Ф.И.О)

«___» _____________ 201__ г.

<ФИО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ, ДОЛЖНОСТЬ, ОТДЕЛ, УПРАВЛЕНИЕ>

_________________/__________________
(подпись) (Ф.И.О)

«___» _____________ 201__ г.

Приложение №21. Заключение о возможности эксплуатации СКЗИ

ЗАКЛЮЧЕНИЕ
о возможности эксплуатации средств криптографической защиты информации

г._____ «___» _____ 20__ г.

По результатам проверки готовности обладателя конфиденциальной информации <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ> к самостоятельному использованию СКЗИ <НАИМЕНОВАНИЕ СКЗИ>, установлено:

1. На основании акта(ов) готовности от __.__.20__ г. №__ АРМ согласно Таблице 1 соответствуют требованиям 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 13.06.2001 №152 и готов(ы) к эксплуатации.

Таблица 1

№ п/п	Учетный номер АРМ	№ печати

2. Пользователи СКЗИ <НАИМЕНОВАНИЕ СКЗИ> (Таблица 2) обучены правилам работы с СКЗИ и допущены к самостоятельной работе с СКЗИ согласно Таблице №2.

Таблица 2

№ п/п	ФИО пользователя СКЗИ

Эксплуатацию СКЗИ <НАИМЕНОВАНИЕ СКЗИ> разрешаю до «___» _____ 20__ г[1]

Начальник отдела
криптографической защиты
АО «Гринатом» _____/_____
(подпись) (ФИО)

М.П.

[1] В случае сохранения доверенной среды функционирования СКЗИ, подтвержденной Актом(ами), указанными в Заключении.

Приложение №22. Журнал выполнения регламентных работ

ЖУРНАЛ
учета выполнения регламентных работ
<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

Дата	Наименование работы и причина ее выполнения	Должность, фамилия и подпись		Примечание
		Выполнившего работу	Проверившего работу	

Приложение №23. Порядок проведения расследований фактов нарушения условий использования СКЗИ

ПОРЯДОК

проведения расследований фактов нарушения условий использования средств криптографической защиты информации в организациях Госкорпорации «Росатом»

Москва 2020 г.

Оглавление

1. Назначение и область применения

Настоящий Порядок проведения расследований[1] фактов нарушения условий использования средств криптографической защиты информации (далее – СКЗИ) в организациях-обладателях конфиденциальной информации (далее – ООКИ, далее – Порядок) разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты и предназначен для упорядочения и повышения эффективности деятельности при:

создании и организации работы Комиссий по расследованию фактов нарушения условий использования СКЗИ (далее – Комиссии);

проведении расследований фактов нарушения условий использования СКЗИ (далее – Расследования), выработке предупреждающих действий (профилактических мер) и принятии решений по их реализации.

Порядок является локальным нормативным документом, который регламентирует создание Комиссий, организацию их деятельности по проведению Расследований в ООКИ.

Порядок описывает подпроцесс «Расследование фактов нарушений условий использования СКЗИ» процесса «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Требования настоящего Порядка обязательны для исполнения в ООКИ, заключившими с лицензиатом ФСБ России АО «Гринатом» договор на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств (далее – Договор).

Пользователями настоящего Порядка являются сотрудники органа криптографической защиты АО «Гринатом» (далее – ОКЗ) и ООКИ, участвующие в работе Комиссий.

2. Термины, определения и сокращения

В настоящем Порядке используются термины, определения и сокращения из Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – Порядок ОКЗ).

3. Порядок работ

[1] Термин «Расследование» нужно понимать в значении 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, утв. Приказом ФАПСИ № 152 от 13.06.2001 г.

3.1. Организация Расследования

Решение о проведении Расследования в ООКИ принимает одна из сторон по Договору.

Основаниями для создания Комиссии могут являться нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации, а также указания регулятора ФСБ России о необходимости проведения Расследования.

3.2. Порядок формирования Комиссии

Комиссия из числа сотрудников ОКЗ назначается приказом генерального директора АО «Гринатом» о проведении Расследования (далее – Приказ, форма приведена в Приложении №1 к Порядку) в течение десяти рабочих дней после принятия решения одной из сторон по Договору или после поступления указания регулятора ФСБ России о необходимости проведения Расследования.

В Приказе указывается:

ООКИ и причины проведения Расследования;

председатель Комиссии – руководитель ОКЗ;

члены Комиссии - квалифицированные специалисты ОКЗ;

сроки начала и окончания работы Комиссии.

Продолжительность проведения Расследования и состав Комиссии устанавливаются в Приказе, исходя из объёма предстоящих действий по Расследованию, характера и особенностей нарушения, его масштаба и последствий, а также других обстоятельств и не может превышать 30 рабочих дней с момента начала Расследования.

В случае необходимости дополнительной проверки обстоятельств нарушения условий использования СКЗИ, в том числе связанной с проведением технических и иных экспертиз, решение о продлении срока Расследования принимается генеральным директором АО «Гринатом» по представлению председателя Комиссии.

3.3. Порядок работы Комиссии

3.3.1. В течение трех дней после подписания Приказа ОКЗ письмом уведомляет руководителя ООКИ, в которой произошло нарушение условий использования СКЗИ, о предстоящем расследовании. Для проведения Расследования члены Комиссии в течение девяти дней после подписания Приказа командируются в ООКИ, в которой произошло подлежащее Расследованиюнарушение условий использования СКЗИ.

Расследование начинается с ознакомления руководителя ООКИ с основаниями, целями, порядком, сроками и условиями проведения Расследования.

Под руководством председателя Комиссии перед началом основных мероприятий по Расследованию проводится совместное совещание членов Комиссии и должностных лиц ООКИ.

На совещании руководитель ООКИ представляет следующие материалы:

акты предыдущих (за последние три года) проверок ФСБ России и/или ОКЗ условий использования СКЗИ в ООКИ;

планы реализации рекомендаций по результатам проверок ФСБ России и/или ОКЗ.

На совещании проводится заслушивание должностных лиц ООКИ, ответственных за организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, а также руководителей подразделений ООКИ, в которых произошли нарушения условий использования СКЗИ и/или имеются последствия нарушений. Обсуждается план работы Комиссии (форма плана работы Комиссии приведена в Приложении №3 к настоящему Порядку).

3.3.2. Расследование фактов нарушения условий использования СКЗИ проводится в соответствии с планом работы Комиссии, который оформляется в первый день работы Комиссии. План работы Комиссии согласовывается с руководителем ООКИ и утверждается председателем Комиссии.

В плане работы Комиссии указываются:

наименование подразделений и СКЗИ, подлежащих проверке и (или) обследованию;

направления расследования и конкретные вопросы, ответы на которые необходимо получить в ходе расследования;

фамилия, имя, отчество члена Комиссии, уполномоченного на проведение расследования конкретного вопроса, сроки его проведения;

даты начала и окончания проведения расследования;

перечень документов, представляемых ООКИ в ходе расследования;

перечень отчётных документов и/или материалов, содержащих результаты расследования.

3.3.3. Руководитель ООКИ должен обеспечить:

представление документов по вопросам Расследования,

подготовку протоколов опросов очевидцев нарушения условий использования СКЗИ и должностных лиц ООКИ,

в установленном порядке доступ лиц, осуществляющих Расследование, к проверяемым СКЗИ и к сведениям, составляющим конфиденциальную информацию, в случае необходимости.

3.3.4. Комиссией принимаются к рассмотрению только официально зарегистрированные документы, после чего с них снимаются заверенные копии, делаются выписки.

Количество и состав документов и материалов, представляемых ООКИ, определяется и уточняется председателем Комиссии в ходе работы Комиссии.

Все работники ООКИ обязаны оказывать содействие работе Комиссии. Лица, препятствующие расследованию, отстраняются от взаимодействия с Комиссией руководителем ООКИ по ходатайству председателя Комиссии.

Изъятие документации во время проведения расследования оформляется описью (форма Описи документов приведена в Приложении №4 к настоящему Порядку), подписанной председателем и членами Комиссии, а также должностными лицами ООКИ, ответственными за хранение изымаемой документации.

3.3.5. В ходе расследования членами Комиссии выполняются мероприятия, определенные планом работы Комиссии, в том числе:

осмотр и фотографирование, а в необходимых случаях – видеосъемка, оформление протоколов осмотра места нарушения условий использования СКЗИ;

опрос очевидцев, должностных лиц и получение от них письменных объяснений;

выяснение обстоятельств, предшествовавших нарушению условий использования СКЗИ, установление причин их возникновения;

оценка достаточности соблюдения установленных требований по использованию СКЗИ для предупреждения нарушения условий использования СКЗИ;

проверка квалификации администраторов безопасности, обслуживающих СКЗИ, условия использования которых были нарушены.

На основе всей совокупности полученных данных членами Комиссии:

устанавливаются причины нарушения условий использования СКЗИ и сценарий их развития,

определяются лица, ответственные за допущенные нарушения условий использования СКЗИ,

предлагаются корректирующие меры по устранению причин нарушения условий использования СКЗИ, предупреждению повторения нарушений.

3.3.6. При наличии подозрений на причинение вреда от нарушения условий использования СКЗИ ООКИ может осуществить расчет причиненного вреда (экономического ущерба), расчет подписывается руководителем и главным бухгалтером ООКИ.

Расчет вреда (экономического ущерба), если он произведен, прилагается к Заключению по результатам расследования фактов нарушения условий использования СКЗИ (далее – Заключение, форма Заключения приведена в Приложении №2 к настоящему Порядку).

3.3.7. Действия членов Комиссии при Расследовании не должны нарушать деятельность и обеспечение информационной безопасности в ООКИ.

3.3.8. Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то председатель Комиссии вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений.

3.4. Оформление и учет материалов расследования, организация устранения причин нарушения условий использования СКЗИ

3.4.1. Результаты работы Комиссии оформляются Заключением.

Заключение состоит из вводной, описательной, заключительной частей и приложений.

Вводная часть Заключения содержит следующую информацию:

основание для Расследования;

полное наименование ООКИ и СКЗИ, правила использования которого были нарушены,

должности, фамилии, имена, отчества должностных лиц (председателя, заместителя председателя и членов Комиссии), проводивших расследование,

даты начала и окончания расследования,

перечень подразделений и должностных лиц ООКИ, участвовавших в мероприятиях по расследованию.

Описательная часть Заключения содержит сведения об СКЗИ, о проведенных мероприятиях по расследованию и их результатах, в том числе о выявленных нарушениях условий использования СКЗИ и, при необходимости, иные дополнительные сведения, подтверждающие результаты расследования и выводы Комиссии.

Заключительная часть Заключения содержит выводы по установлению обстоятельств и причин нарушения условий использования СКЗИ с указанием:

перечня должностных лиц, допустивших нарушения,

принятых мер по ликвидации последствий нарушения,

продолжительности простоя и материальном (экономическом) ущербе (если расчет производился). Здесь же формулируются предложения по устранению причин и последствий нарушения, а также по организационным мероприятиям для предупреждения и профилактики аналогичных нарушений в работе данного и других СКЗИ.

3.4.2. К Заключению оформляются следующие приложения:

копия Приказа,

протокол осмотра места нарушения условий использования СКЗИ с необходимыми фото- и видеоматериалами,

протоколы опроса очевидцев и объяснения лиц, причастных к нарушению условий использования СКЗИ, а также должностных лиц, ответственных за соблюдение условий использования СКЗИ,

копии протоколов и удостоверений об обучении и аттестации администраторов безопасности и пользователей СКЗИ, обслуживающих и работающих с СКЗИ,

справки о размере причиненного вреда и оценке экономического ущерба от нарушения условий использования СКЗИ (если расчет производился),

сведения о нарушениях требований законодательных и нормативных технических документов (перечень нарушений требований информационной безопасности, выявленных в ходе расследования),

предложения Комиссии по проведению соответствующих компенсирующих мероприятий,

другие материалы, характеризующие нарушение условий использования СКЗИ, обстоятельства и причины возникновения нарушения, его развитие, последствия.

Перечень материалов, прилагаемых к Заключению может изменяться и дополняться по письменному решению председателя Комиссии в зависимости от характера и обстоятельств нарушения. Таким решением может быть запрос к руководителю ООКИ о предоставлении Комиссии дополнительных материалов. Указанное решение также оформляется в виде приложения к Заключению.

3.4.3. Результаты расследования, содержащие сведения, составляющие конфиденциальную информацию, оформляются с соблюдением требований, предусмотренных законодательством Российской Федерации о защите конфиденциальной информации.

3.4.4. Заключение после завершения работы Комиссии составляется в двух экземплярах, подписывается всеми членами Комиссии и председателем Комиссии, представляется для ознакомления руководителю управления информационной безопасности АО «Гринатом» и после подписания им два экземпляра направляются руководителю ООКИ для ознакомления и подписания. Один экземпляр Заключения остается в ООКИ, один возвращается в ОКЗ.

В АО «Гринатом» Заключения, а также все иные документы, возникшие в ходе расследования, помещаются в дела и хранятся согласно Инструкции по делопроизводству и сводной номенклатуре дел АО «Гринатом».

В ООКИ документы, возникшие в ходе расследования, помещаются в дела и хранятся согласно сводной номенклатуре дел ООКИ и локальному нормативному акту ООКИ, регламентирующему хранение документов.

3.4.5. Руководитель ООКИ, в которой произошло нарушение условий использования СКЗИ, в течение десяти рабочих дней с момента ознакомления с Заключением утверждает План устранения недостатков по результатам проведения расследования нарушения условий использования СКЗИ (далее – План устранения недостатков, форма Плана устранения недостатков представлена в приложении №33 к Порядку ОКЗ).

3.4.6. Копия плана устранения недостатков в течение трех рабочих дней после его утверждения направляется руководителем ООКИ в ОКЗ.

3.4.7. Руководитель ООКИ в случае несогласия с фактами и выводами, изложенными в Заключении, в течение десяти рабочих дней от даты получения экземпляра Заключения вправе представить руководителю ОКЗ в письменной форме возражения в отношении Заключения в целом или в отношении отдельных положений. При этом он вправе приложить к своим возражениям документы, подтверждающие обоснованность возражений, или их заверенные копии.

3.4.8. Результаты выполнения Плана устранения недостатков ежеквартально оформляются в виде отчётов в произвольной форме, подписываются руководителем ООКИ и направляются в ОКЗ.

4. Нормативные ссылки

Приказ ФАПСИ № 152 от 13.06.2001 г. «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».

5. Внесение изменений в Порядок

Инициатором и координатором работ по изменению Порядка является ОКЗ.

В случае если инициатором изменений выступает не ОКЗ, то инициатор внесения изменений должен представить ОКЗ обоснование практической целесообразности таких изменений.

Изменения Порядка после оценки их целесообразности проходят процедуру согласования в установленном порядке. При внесении изменений утверждается новая редакция Порядка.

6. Контроль и ответственность

Ответственность за выполнение требований Порядка возлагается на сотрудников ОКЗ и ООКИ, участвующих в работе Комиссий.

Контроль выполнения требований Порядка возлагается на ОКЗ.

За бездействие (халатность) при проведении Расследования, а также за недостоверность и несвоевременность передаваемой в ходе Расследования информации члены Комиссии, экспертные специалисты, привлекаемые к работе Комиссии, работники организаций, привлекаемые к Расследованию, несут ответственность в соответствии с действующим законодательством, нормативными правовыми актами Российской Федерации и локальными нормативными актами Государственной корпорации по атомной энергии «Росатом» и ООКИ.

Приложение №1 к Порядку. Форма Приказа о проведении Расследования

Акционерное общество «Гринатом»

« » 20 г. Москва № _____

(дата)

О проведении расследования обстоятельств и причин нарушения условий использования средств криптографической защиты информации в

_____

(наименование организации)

В соответствии с Порядком проведения расследований фактов нарушения условий использования средств криптографической защиты информации Госкорпорации «Росатом» и ее организациях, утв. в рамках договора присоединения от 06 июля 2012 г. на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств:

1. Назначить комиссию по проведению расследования обстоятельств и причин нарушения условий использования СКЗИ в (на):

_____

(наименование объекта)

в составе:

Фамилия И.О._____, председатель комиссии

(должность)

(руководитель ОКЗ),

Фамилия И.О._____,

(должность)

Фамилия И.О._____.

(должность)

2. Комиссии в период с «___»_____ 20___ г. по «___»_____ 20___ г. провести расследование обстоятельств и причин нарушения условий использования СКЗИ в _____

(наименование организации)

в установленном порядке.

3. Контроль за исполнением настоящего Приказа возложить на руководителя Органа криптографической защиты АО «Гринатом» _____ .

(Фамилия И.О.)

Генеральный директор _____/_____

(подпись) (И.О. Фамилия)

Приложение №2 к Порядку. Форма заключения по результатам Расследования

УТВЕРЖДАЮ	**ОЗНАКОМЛЕН**
<ДОЛЖНОСТЬ ПРЕДСЕДАТЕЛЯ КОМИССИИ (РУКОВОДИТЕЛЯ ОКЗ), НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАНСОСТИ АО «ГРИНАТОМ»>
_____/_____	_____/_____
(подпись) (Ф.И.О)	(подпись) (Ф.И.О)
«___»_____ 20__ г.	«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
комиссии Органа криптографической защиты АО «Гринатом»
по результатам расследования фактов
нарушения условий использования СКЗИ в
<ПОЛНОЕ НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

СОГЛАСОВАНО	СОГЛАСОВАНО	ОЗНАКОМЛЕН
<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>	<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ ООКИ>
_____/_____	_____/_____	_____/_____
(подпись) (Ф.И.О)	(подпись) (Ф.И.О)	(подпись) (Ф.И.О)
«___»_____ 20__ г.	«___»_____ 20__ г.	«___»_____ 20__ г.

Во исполнение Приказа АО «Гринатом» от «___» _____ 20___ г. о проведении расследования фактов нарушения условий использования СКЗИ и в соответствии с Договором Присоединения от 06 июля 2012 г. №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств (заявление о присоединении от «___» _____ 201__ г. №_____) в период с «___» по «___» _____ 201__ г. комиссией в составе:

1. Председатель комиссии: <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ПРЕДСЕДАТЕЛЯ КОМИССИИ>,
2. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ЧЛЕНА КОМИССИИ>
3. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ, ФИО ЧЛЕНА КОМИССИИ>

проведено расследование фактов нарушения условий использования СКЗИ <НАИМЕНОВАНИЕ СКЗИ> в <ПОЛНОЕ НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>.

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с 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 июня 2001г. №152 (далее – Инструкция №152).

5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.
12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

Сотрудники ООКИ:

1. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ООКИ, ФИО>,
2. <ДОЛЖНОСТЬ, НАИМЕНОВАНИЕ ООКИ, ФИО>,

.

.

СКЗИ и оборудование, в составе которого оно эксплуатируется:

1. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,
2. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,
3. <НАИМЕНОВАНИЕ СКЗИ, МЕСТОРАСПОЛОЖЕНИЕ АРМ с СКЗИ, S/N АРМ, НАИМЕНОВАНИЕ И ВЕРСИЯ ОС И ПР.>,

ПРОВЕРКОЙ УСТАНОВЛЕНО

_____

_____

_____

(сведения об СКЗИ, о проведенных мероприятиях по расследованию и их результатах, в том числе о выявленных нарушениях условий использования СКЗИ и иные дополнительные сведения, подтверждающие результаты расследования и выводы Комиссии)

УКАЗАНИЯ И РЕКОМЕНДАЦИИ

.

.

ВЫВОДЫ

1. <ОБСТОЯТЕЛЬСТВА И ПРИЧИНЫ НАРУШЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СКЗИ>,
2. <ПЕРЕЧЕНЬ ДОЛЖНОСТНЫХ ЛИЦ, ДОПУСТИВШИХ НАРУШЕНИЯ>,
3. <ПРОДОЛЖИТЕЛЬНОСТЬ ПРОСТОЯ И МАТЕРИАЛЬНЫЙ (ЭКОНОМИЧЕСКИЙ) УЩЕРБ>, если такой расчет производился,
4. <ПРИНЯТЫЕ/НЕОБХОДИМЫЕ МЕРЫ ПО УСТРАНЕНИЮ НАРУШЕНИЙ/ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ НАРУШЕНИЙ>.

Приложение №3 к Порядку. Форма плана работы Комиссии

ПЛАН

работы комиссии по расследованию фактов нарушения условий использования СКЗИ в

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

№ п/п	Наименование подразделения, местонахождение АРМ с СКЗИ, должность, ФИО пользователя СКЗИ в зоне ответственности которого находятся СКЗИ, условия использования которых были нарушены	Вопросы/ направления расследования	Перечень документов представляемых ООКИ в ходе расследования	Перечень отчетных документов и/или материалов, содержащих результаты расследования	ФИО ответственного члена Комиссии, уполномоченного на проведение расследования конкретного вопроса	Срок проведения расследования конкретного вопроса	Отметка о проведении расследования (выполнено/не выполнено)

Дата начала расследования: «___» _____ 201__ г.

Дата окончания расследования: «___» _____ 201__ г.

«УПОЛНОМОЧЕННОЕ ДОЛЖНОСТНОЕ ЛИЦО ООКИ,
НАИМЕНОВАНИЕ ООКИ»

_____/_____
(подпись) (Ф.И.О)

Председатель Комиссии

_____/_____
(подпись) (Ф.И.О)

Приложение №4 к Порядку. Форма описи документов

ОПИСЬ ДОКУМЕНТОВ

Настоящим удостоверяется, что _____
(Ф.И.О., должность, наименование ООКИ)
представил, а Комиссия в лице _____
(Ф.И.О., должность, наименование ООКИ)
приняла следующие документы для проведения расследования фактов нарушений условий использования СКЗИ.

№ п/п	Наименование документа	Количество листов	Дополнительные сведения
1			
2			
3			
Всего:			

Документы сдал: _____/_____
(подпись) (Ф.И.О)

Председатель Комиссии: _____/_____
(подпись) (Ф.И.О)

Члены комиссии:

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

Приложение №24. Акт уничтожения СКЗИ

АКТ
уничтожения СКЗИ
№ ____

г. _____ « ___ » _____ 20 ___ г.

Комиссия из числа сотрудников органа криптографической защиты в составе:

1. _____
(ФИО, должность)
2. _____
(ФИО, должность)
3. _____
(ФИО, должность)

назначенных приказом от _____ г. № _____ в <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ> составила настоящий акт о том, что перечисленные в нем СКЗИ, указанные в таблице №1, уничтожены путем <СПОСОБ УНИЧТОЖЕНИЯ>.

Таблица №1

№ п/п	**Наименование СКЗИ**	**Уч. №АРМ**	**Серийный номер сертификата ключа проверки электронной подписи / номер лицензии**	**ФИО пользователя СКЗИ**

Уничтожено в количестве _____ (цифрами и прописью) наименований и экземпляров ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации.

Члены комиссии:

_____/_____
(подпись) (Ф.И.О)

_____/_____
(подпись) (Ф.И.О)

Приложение №25. Приказ о проведении проверки

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»

П Р И К А З

« » _____ 20__ г. Москва №_____

О проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

В рамках оказания услуги CLB.18 по договору №22/2143-Д от 06.07.2012 для осуществления контроля за организацией и обеспечением безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну:

ПРИКАЗЫВАЮ:

1. Утвердить план-график проведения проверок на 20__ год (Приложение № 1).
2. Работникам отдела криптографической защиты <ФАМИЛИЯ И.О.> и <ФАМИЛИЯ И.О.> провести проверку организации и обеспечения безопасности хранения, обработки и передачи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, согласно плану-графику проведения проверок на 20__ год.
3. Контроль исполнения настоящего приказа возложить на «ДОЛЖНОСТЬ, ФАМИЛИЯ И.О. УПОЛНОМОЧЕННОГО ЛИЦА».

Генеральный директор <И.О. ФАМИЛИЯ>

Приложение №26. План-график проведения проверок

Приложение №1
УТВЕРЖДЕН
приказом АО «Гринатом»
от _____№_____

План-график проведения проверок на 20__ год

№ п/п	Предприятие	Адрес месторасположения	Проверяющие	Срок проведения проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну	Кол-во СКЗИ (на момент составления приказа)

Приложение №27. Информационное письмо о проведении проверки

Акционерное общество «Гринатом»
(АО «Гринатом»)

1-й Нагатинский проезд, д. 10, стр. 1,
Москва, 115230
Телефон (499) 949-49-19, факс (499) 949-44-46
E-mail: info@greenatom.ru
ОКПО 64509942, ОГРН 1097746819720
ИНН 7706729736, КПП 770601001

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА»
«НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

«И.О.ФАМИЛИЯ»

_____ № _____

На № _____ от _____

О проведении проверки работ по договору №22/2143-Д от 06.07.2012 г.

Уважаемый(-ая) «ИМЯ ОТЧЕСТВО»!

В рамках договора №22/2143-Д от 06.07.2012 г, заявлений на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (услуга CLB.18) и заявлений на создание квалифицированных сертификатов ключей проверки электронной подписи (услуга CLB.11) в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ» выданы СКЗИ в количестве _____ед. и квалифицированные сертификаты ключей проверки электронной подписи в количестве _____ед.

Приказом от __.__.201_ г. № _____ о проведении проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну возложено на специалистов лицензиата ФСБ России АО «Гринатом» и утверждён план-график проведения проверок.

Прошу согласовать время и дату проведения проверки в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ» и обеспечить доступ к СКЗИ.

Время	Дата	Количество СКЗИ	Количество ключей проверки ЭП	Исполнитель (должность, Ф.И.О)

С уважением,
Начальник отдела криптографической защиты И.О. Фамилия
(по дов. № _____ от _____)

Исп.:
Тел.:

Приложение №28. Сводная таблица по объекту проверки

Сводная таблица по <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ	**ВЫПОЛНЕНО/ ВЫПОЛНЕНО ЧАСТИЧНО/ НЕ ВЫПОЛНЕНО, КОММЕНТАРИЙ**
Сотрудники ОКЗ/администраторы безопасности	
Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ): – наличие Приказа, – включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности, – включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.	
Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ: – наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам	
Наличие обязанностей администратора безопасности в	

должностных инструкциях сотрудников, выполняющих эти обязанности	
Ознакомление под расписку с 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 июня 2001г. №152 (далее – Инструкция №152)	
Наличие у администраторов безопасности личных металлических печатей	
Помещение ОКЗ/помещение администраторов безопасности	
Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ: – наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ; – наличие опечатывающих устройств на дверях спецпомещений ОКЗ; – наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время; – наличие ключей и их дубликатов от дверей спецпомещений ОКЗ; – учет ключей и их дубликатов от дверей спецпомещений ОКЗ в	

журнале учета хранилищ и ключей; – порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам	
– Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей: – наличие металлических хранилищ; – наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ; – наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ; – учет металлических хранилищ в журнале учета хранилищ и ключей; – учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей; – порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня; – порядок сдачи ключей от металлического хранилища ответственного должностного	

лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам	
– Окна спецпомещений ОКЗ: – наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц; – наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ	
– Документация ОКЗ	
– Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность	
– Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность	
– Выписка из номенклатуры дел	
– Журнал учета хранилищ и ключей	

– Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них	
– Журнал учета печатей и штампов	
– Журнал учета электронных носителей информации, содержащих конфиденциальную информацию	
– Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета): – наличие журналов поэкземплярного учета; – учет журналов поэкземплярного учета в номенклатуре дел; – правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.); – актуальность информации в журналах поэкземплярного учета	
Акты готовности СКЗИ к эксплуатации (далее – Акты): – наличие Актов; – правильность составления Актов; – актуальность информации в Актах	
Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения: – наличие заключений о сдаче зачетов; – правильность составления заключений; – актуальность информации в заключениях о сдаче зачетов	

Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность	
Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация	
Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ	
Помещения с установленными СКЗИ	
Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ: – наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ; – наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ; – наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время; – наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ; – учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей; – порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или	

дежурному по организации по окончании рабочего дня; – отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.	
Шкафы (ящики, хранилища) индивидуального пользования: – наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования; – наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования; – учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей; – учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ; – отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам	
Окна спецпомещений пользователей СКЗИ: – наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение	

в спецпомещения пользователей СКЗИ посторонних лиц; – наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ	
Пользователи СКЗИ	
Наличие у пользователей СКЗИ ключевых документов	
Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ)	
Знания пользователями требований при работе с СКЗИ	
Выполнение пользователями требований при работе с СКЗИ	
АРМ пользователей СКЗИ	
Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах	
Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах	
Наличие СКЗИ на АРМ пользователей;	
Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ	
Наличие на АРМ с СКЗИ сертифицированных антивирусных средств	
Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД)	
Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на	

удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ	
Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей	

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

№ п/п	АРМ проверен/не проверен	№ сертификата	Дата окончания сертификата	ФИО пользователя СКЗИ	Наименование СКЗИ	Серийный номер СКЗИ			Номер АРМ				Номер печати на АРМ			Обучение пользователей СКЗИ			Приказ о допуске		СЗИ от НСД	Антивирус	Права учетной записи	Аттестат соответствия
						Схема КЗ	ЖПУ	Фактическое состояние	Схема КЗ	Акт готовности	ЖПУ	Фактическое состояние	Схема КЗ	Акт готовности	Фактическое состояние	Схема КЗ	Заключение о сдаче зачетов	Фактическое состояние	Схема КЗ	Фактическое состояние				

Приложение №29. Программа проверки

ПРОГРАММА
проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в

_____
<Наименование организации>

ЦЕЛЬ ПРОВЕРКИ:

В рамках договора №22/2143-Д от 06.07.2012 осуществление контроля за реализацией требований Порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

ПРОВЕРЯЕМЫЕ ВОПРОСЫ:

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с 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 июня 2001г. №152 (далее – Инструкция №152).
5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.

12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств,

препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

ОСНОВАНИЕ ДЛЯ ПРОВЕРКИ: _____

ВРЕМЯ ПРОВЕДЕНИЯ ПРОВЕРКИ: «__» _____ - «__» _____ 20__ года

ПРОГРАММА-ГРАФИК ПРОВЕРКИ:

№ п.п.	Вид выполняемых работ	Срок выполнения, ответственный
1	**Подготовка к проверке**	

1.1	Изучение материалов по объекту проверки: • выписка из Схемы организации криптографической защиты конфиденциальной информации; • выписка из Центра Регистрации Удостоверяющего центра Госкорпорации «Росатом». Уточнение перечня объектов, подлежащих проверке: • перечень СКЗИ; • перечень сертификатов ключей проверки электронной подписи.	
1.2.	Подготовка сводной таблицы по объекту проверки.	
2	**Проведение проверки**	
2.1	• Прибытие на предприятие; • Встреча с руководителем, проведение установочного совещания (разъяснение цели проверки); • Проверка сотрудников ОКЗ/администраторов безопасности; • Проверка помещения(ий) ОКЗ/помещения(ий) администраторов безопасности; • Проверка документации ОКЗ.	
2.2	• Проверка помещений с установленными СКЗИ; • Проверка пользователей СКЗИ; • Проверка АРМ пользователей СКЗИ.	
3	**Подведение итогов проверки**	
3.1	Формирование акта проверки и отправка на предприятие	

Начальник отдела криптографической защиты _____/_____
(подпись) (Ф.И.О)

Начальник Управления информационной безопасности _____/_____
(подпись) (Ф.И.О)

Приложение №30. Акт проверки

Рег. № _____
от _____

Для служебного пользования
(п. ____, ____ Перечня ДСП)
Экз №__

УТВЕРЖДАЮ

<ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ ПРОВЕРКИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ОЗНАКОМЛЕН

<ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

АКТ
проверки организации и обеспечения безопасности информации с использованием средств криптографической защиты в

_____
<Наименование организации>

СОГЛАСОВАНО

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

СОГЛАСОВАНО

<ДОЛЖНОСТЬ ЧЛЕНА КОМИССИИ, НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

В соответствии с Приказом АО «Гринатом»[1] от _____ №_____ «О проведении проверок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» органа криптографической защиты АО «Гринатом» (далее – ОКЗ) в период с «___» по «___»_____ 20__ г. комиссией в составе:

1. <ФИО ПРОВЕРЯЮЩЕГО>,
2. <ФИО ПРОВЕРЯЮЩЕГО>.

проведена проверка организации работ и состояния защиты с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее – защита информации) в <НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>, расположенном по адресу: _____.

ПРОВЕРКЕ ПОДВЕРГАЛИСЬ

Сотрудники ОКЗ/администраторы безопасности

1. Приказ о назначении администраторов безопасности и лиц, их замещающих (далее – Приказ):

наличие Приказа,

включение в Приказ всех сотрудников, выполняющих обязанности администратора безопасности,

включение администраторов безопасности в состав комиссии по составлению заключений на основании принятых от пользователей средств криптографической защиты информации (далее - СКЗИ) зачетов по программе обучения правилам работы с СКЗИ, а также по уничтожению СКЗИ и ключевых документов.

2. Уровень квалификации администратора безопасности для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ:

наличие у администратора безопасности подтверждения об обучении и/или повышении квалификации в организации, имеющей лицензию на ведение образовательной деятельности по соответствующим программам.

---

[1] Лицензия от 19.01.2017 ЛСЗ №0014254 Рег.№15686 на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

3. Наличие обязанностей администратора безопасности в должностных инструкциях сотрудников, выполняющих эти обязанности.

4. Ознакомление под расписку с 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 июня 2001г. №152 (далее – Инструкция №152).

5. Наличие у администраторов безопасности личных металлических печатей.

Помещение ОКЗ/помещение администраторов безопасности

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения, где хранятся СКЗИ, эксплуатационная и техническая документация к ним (далее – спецпомещения ОКЗ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения ОКЗ,

наличие опечатывающих устройств на дверях спецпомещений ОКЗ,

наличие замков на дверях спецпомещений ОКЗ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений ОКЗ,

учет ключей и их дубликатов от дверей спецпомещений ОКЗ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений ОКЗ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений ОКЗ ответственным должностным лицам.

2. Металлические хранилища для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей:

наличие металлических хранилищ,

наличие внутренних замков и кодовых замков или приспособлений для опечатывания замочных скважин металлических хранилищ,

наличие ключей и дубликатов ключей (как минимум двух экземпляров) от металлических хранилищ,

учет металлических хранилищ в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от металлических хранилищ в журнале учета хранилищ и ключей,

порядок сдачи ключей от металлических хранилищ ответственному должностному лицу по окончании рабочего дня,

порядок сдачи ключей от металлического хранилища ответственного должностного лица, где хранятся ключи от всех остальных хранилищ, в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от металлических хранилищ ответственным должностным лицам.

3. Окна спецпомещений ОКЗ:

наличие металлических решеток или ставней на окнах спецпомещений ОКЗ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения ОКЗ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения ОКЗ посторонних лиц,

наличие на окнах спецпомещений ОКЗ приспособлений для предотвращения просмотра извне спецпомещений ОКЗ.

Документация ОКЗ

1. Наличие утвержденного перечня лиц, допускаемых к самостоятельной работе с СКЗИ и его актуальность;
2. Наличие утвержденного Приказа о предоставлении прав подписей в системах (для банковских платежных систем) и его актуальность;
3. Выписка из номенклатуры дел.
4. Журнал учета хранилищ и ключей.
5. Журнал учета приема (сдачи) под охрану специальных помещений и ключей от них,
6. Журнал учета печатей и штампов.
7. Журнал учета электронных носителей информации, содержащих конфиденциальную информацию.
8. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – журналы поэкземплярного учета):

наличие журналов поэкземплярного учета,

учет журналов поэкземплярного учета в номенклатуре дел,

правильность ведения журналов поэкземплярного учета (прошит/не прошит, наличие нумерации, правильность заполнения граф и пр.),

актуальность информации в журналах поэкземплярного учета.

9. Акты готовности СКЗИ к эксплуатации (далее – Акты):

наличие Актов,

правильность составления Актов,

актуальность информации в Актах.

10. Заключения о сдаче зачетов, составленные на основании принятых от пользователей СКЗИ зачетов по программе обучения:

наличие заключений о сдаче зачетов,

правильность составления заключений,

актуальность информации в заключениях о сдаче зачетов.

11. Наличие Заключений о возможности эксплуатации СКЗИ и их актуальность.
12. Заключения ПДТК на объекты информатизации, где установлены СКЗИ, но не обрабатывается конфиденциальная информация.

13. Аттестаты соответствия ФСТЭК на объекты информатизации с установленными СКЗИ.

Помещения с установленными СКЗИ

1. Утвержденные правила допуска сотрудников и посетителей в рабочее и нерабочее время в помещения с установленными СКЗИ (далее – спецпомещения пользователей СКЗИ), исключающие возможность неконтролируемого проникновения или пребывания посторонних лиц, а также просмотр посторонними лицами ведущихся там работ:

наличие утвержденных перечней лиц, допускаемых в спецпомещения пользователей СКЗИ,

наличие опечатывающих устройств на дверях спецпомещений пользователей СКЗИ,

наличие замков на дверях спецпомещений пользователей СКЗИ, гарантирующих надежное закрытие в нерабочее время,

наличие ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ,

учет ключей и их дубликатов от дверей спецпомещений пользователей СКЗИ в журнале учета хранилищ и ключей,

порядок сдачи ключей от дверей спецпомещений пользователей СКЗИ в службу охраны или дежурному по организации по окончании рабочего дня,

отметки о выдаче ключей и дубликатов ключей от спецпомещений пользователей СКЗИ ответственным должностным лицам.

2. Шкафы (ящики, хранилища) индивидуального пользования:

наличие надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования,

наличие приспособлений для опечатывания замочных скважин на шкафах (ящиках, хранилищах) индивидуального пользования,

учет шкафов (ящиков, хранилищ) в журнале учета хранилищ и ключей,

учет ключей и дубликатов ключей от шкафов (ящиков, хранилищ) в журнале учета хранилищ,

отметки о выдаче ключей и дубликатов ключей от шкафов (ящиков, хранилищ) ответственным должностным лицам.

3. Окна спецпомещений пользователей СКЗИ:

наличие металлических решеток или ставней на окнах спецпомещений пользователей СКЗИ, или охранной сигнализации, или других средств, препятствующих неконтролируемому проникновению в спецпомещения пользователей СКЗИ, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения пользователей СКЗИ посторонних лиц,,

наличие на окнах спецпомещений пользователей СКЗИ приспособлений для предотвращения просмотра извне спецпомещений пользователей СКЗИ.

Пользователи СКЗИ

1. Наличие у пользователей СКЗИ ключевых документов.
2. Наличие печатей у пользователей СКЗИ для опечатывания шкафов (ящиков, хранилищ).
3. Знания пользователями требований при работе с СКЗИ.
4. Выполнение пользователями требований при работе с СКЗИ.

АРМ пользователей СКЗИ

1. Наличие и соответствие учетных (серийных) номеров АРМ пользователей СКЗИ с номерами, указанными в ЖПУ и Актах.
2. Наличие и соответствие номеров средств контроля за вскрытием АРМ (печатей, пломб) с установленными СКЗИ с номерами, указанными в Актах.
3. Наличие СКЗИ на АРМ пользователей,
4. Актуальность сертификатов соответствия ФСБ на СКЗИ, установленные на АРМ пользователей СКЗИ.
5. Наличие на АРМ с СКЗИ сертифицированных антивирусных средств.
6. Наличие на АРМ с СКЗИ сертифицированных средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).
7. Права пользователей СКЗИ на АРМ с СКЗИ (на учетные записи, на антивирусы, на СЗИ от НСД), права на удаленное администрирование и модификацию ОС и ее настроек на АРМ с СКЗИ.
8. Максимальные сроки действия паролей к учетным записям на АРМ с СКЗИ, параметры автоматической блокировки учетных записей.

ПРОВЕРКОЙ УСТАНОВЛЕНО

Услуги по защите информации в осуществляет АО «Гринатом» в соответствии с договором присоединения от 06.07.2012 г. №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств (заявление о присоединении от _____ № _____, далее – Договор).

Объем работ по договорам на дату проверки:

1.	CLB.11	Предоставление услуг Удостоверяющего центра	___ ед.
2.	CLB.18	Обеспечение безопасности информации с использованием средств криптографической защиты информации	___ ед.
3.	GEN.23	Услуга Администратора безопасности	___ ед.

НАРУШЕНИЯ

Сотрудники ОКЗ/администраторы безопасности

6.1. …
6.2. …

Помещение ОКЗ/помещение администратора безопасности

1. …
2. …

Документация ОКЗ

1. …
2. …

Помещения пользователей СКЗИ

1. …
2. …

Пользователи СКЗИ

1. …
2. …

АРМ пользователей СКЗИ

1. …
2. …

УКАЗАНИЯ И РЕКОМЕНДАЦИИ

Сотрудники ОКЗ/администраторы безопасности

1. …
2. …

Помещение ОКЗ/помещение администратора безопасности

1. …
2. …

Документация ОКЗ

1. …
2. …

Помещения пользователей СКЗИ

1. …
2. …

Пользователи СКЗИ

1. …
2. …

АРМ пользователей СКЗИ

1. …
2. …

ВЫВОДЫ

1. …
2. …

<И.О. ФАМИЛИЯ>
<ТЕЛ>
__ экз. на __ л. каждый:
1 – в адрес
2 – в дело

Приложение №31. План устранения недостатков

«___» _____ 20___ г

ПЛАН

реализации рекомендаций по результатам проверки лицензиата ФСБ России АО «Гринатом»
в «НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

№ п/п	Недостатки, указанные в Акте проверки организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в «Наименование организации»	Рекомендации по устранению выявленных недостатков	Ответственный	Срок	Отметка о выполнении (выполнено/не выполнено)

«ДОЛЖНОСТЬ УПОЛНОМОЧЕННОГО ЛИЦА,
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ»

_____/_____
(подпись) (Ф.И.О)