

Орган криптографической защиты



ГРИНАТОМ

Обучение Администраторов безопасности
Органа криптографической защиты
АО «Гринатом»

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

Соблюдение конфиденциальности информации ограниченного доступа

Реализацию права на доступ к информации

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФАПСИ, лицензиаты ФАПСИ организуют и обеспечивают либо по указанию вышестоящей организации, либо на основании договоров на оказание услуг по криптографической защите конфиденциальной информации.

Лицензиаты ФАПСИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции

При этом лицензиаты ФАПСИ должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты

Федеральный закон от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности»

Основная цель – предотвращение ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации, обороне и безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности.

Статья 2. П2. Задачами лицензирования отдельных видов деятельности являются предупреждение, выявление и пресечение нарушений юридическим лицом, его руководителем и иными должностными лицами, индивидуальным предпринимателем, его уполномоченными представителями (далее - юридическое лицо, индивидуальный предприниматель) требований, которые установлены настоящим Федеральным законом, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.



Соответствие соискателя лицензии этим требованиям является необходимым условием для предоставления лицензии, их соблюдение лицензиатом обязательно при осуществлении лицензируемого вида деятельности.

Постановление Правительства Российской Федерации от 16 апреля 2012 г. N 313*


В Постановлении указаны требования, которые необходимо выполнить для получения лицензии, а также перечислены 28 видов деятельности, работ или услуг, осуществление которых без лицензии ЗАПРЕЩЕНО

Лицензионные требования к АО «Гринатом»:

- ✓ наличие у соискателя лицензии (лицензиата) права собственности или иного законного основания на владение и использование помещений, сооружений, технологического, испытательного, контрольно-измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности;
- ✓ наличие у соискателя лицензии (лицензиата) условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, составляющих лицензируемую деятельность, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";
- ✓ наличие в штате у соискателя лицензии (лицензиата) квалифицированного персонала;

* Положение 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)

Виды деятельности, выполнение которых без лицензии запрещено*


Центр по лицензированию, сертификации и защите
государственной тайны ФСБ России
(наименование лицензирующего органа)

ЛИЦЕНЗИЯ

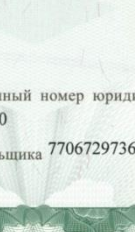
ЛСЗ № 0014254 * Рег. № 15686 Н от « 19 » января 2017 г.

На осуществление (указывается лицензируемый вид деятельности) разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания 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)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности» (указываются в соответствии с перечнем работ (услуг), установленным положением о лицензировании соответствующего вида деятельности):
работы, предусмотренные пунктами 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 21, 22, 23, 24, 25, 26, 27, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

Настоящая лицензия предоставлена (указываются полное и (в случае, если имеется) сокращенное наименование (в том числе фирменное наименование), организационно-правовая форма юридического лица, фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, наименование и реквизиты документа, удостоверяющего его личность)
Акционерному обществу «Гринатом» (АО «Гринатом»)

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1097746819720
Идентификационный номер налогоплательщика 7706729736



Место нахождения и места осуществления лицензируемого вида деятельности (указываются адрес места нахождения (место жительства - для индивидуального предпринимателя) и адреса мест осуществления работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности)

Место нахождения:
119017, г. Москва, ул. Большая Одынка, д. 24

Места осуществления лицензируемого вида деятельности:
Адреса мест осуществления работ, предусмотренных пунктами 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 21, 22, 23, 24, 25, 26, 27, 28 перечня:
119017, г. Москва, ул. Большая Одынка, д. 24;
115230, г. Москва, 1-й Нагатинский пр-д, д. 10, стр. 1.


Адреса мест осуществления работ, предусмотренных пунктами 12, 13, 14, 15, 17, 18, 20, 21, 22, 23, 24, 28 перечня:
427620, Удмуртская Республика, г. Глазов, ул. Белова, д. 7;
624130, Свердловская обл., г. Новоуральск, Центральный проезд, д. 8А, стр. 21;
665816, Иркутская обл., г. Ангарск, ул. 14 Декабря, д. 22;
600007, Владимирская обл., г. Владимир, ул. Северная, д. 1-а, корп.31;
601909, Владимирская обл., г. Ковров, ул. Социалистическая, д. 26, стр.19, корп "И";
663690, Красноярский край, г. Зеленогорск, ул. Первая промышленная, д. 1И/26;
603064, Нижегородская обл., г. Нижний Новгород, проспект Ленина, д. 93;
607188, Нижегородская обл., Дивеевский р-он, пос. Сатис, ул. Парковая, д. 3, зд. 5-1;
630110, Новосибирская обл., г. Новосибирск, ул. Богдана Хмельницкого, д. 94;
636039, Томская обл., г. Северск, ул. Ленина, д. 90;
144001, Московская обл., г. Электросталь, ул. Карла Маркса, д. 12, корп. 75;
191036, г. Санкт-Петербург, ул. 2-я Советская, д. 7.

Настоящая лицензия предоставлена на срок: **бессрочно**


Настоящая лицензия предоставлена на основании решения лицензирующего органа — приказа (распоряжения) от « 19 » января 2017 г. № 27

Настоящая лицензия переоформлена на основании решения лицензирующего органа — приказа (распоряжения) от « _____ » _____ г. № _____

Настоящая лицензия имеет _____ приложение (приложения), являющееся её неотъемлемой частью на _____ листах.



Врио начальника Центра _____ С.А.Финогеев
(подпись уполномоченного лица) (Ф.И.О. уполномоченного лица)



* Постановление Правительства Российской Федерации от 16 апреля 2012 г. N 313



Перечень работ по 313 Постановлению



2. Разработка защищенных с использованием шифровальных (криптографических) средств информационных систем.
3. Разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
7. Производство (тиражирование) шифровальных (криптографических) средств.
8. Производство защищенных с использованием шифровальных (криптографических) средств информационных систем.
9. Производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
10. Производство средств изготовления ключевых документов.
11. Изготовление с использованием шифровальных (криптографических) средств изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах.
- 12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.**
- 13. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем.**
- 14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.**
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
16. Ремонт шифровальных (криптографических) средств.
17. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем.
18. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
- 20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).**
21. Передача шифровальных (криптографических) средств.
22. Передача защищенных с использованием шифровальных (криптографических) средств информационных систем.
23. Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
24. Передача средств изготовления ключевых документов.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
26. Предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
27. Предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации.
28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Орган криптографической защиты

- Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты
- Обладатели конфиденциальной информации, если они приняли решение о необходимости криптографической защиты такой информации или если решение о необходимости ее криптографической защиты в соответствии с Положением ПКЗ-2005 принято государственными органами или государственными организациями, обязаны выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.
- Количество органов криптографической защиты и их численность устанавливает лицензиат ФАПСИ.

Орган криптографической защиты

осуществляет:

- ✓ проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно - программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);
- ✓ разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;
- ✓ обучение лиц, использующих СКЗИ, правилам работы с ними;
- ✓ поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;
- ✓ учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ

Орган криптографической защиты

осуществляет:

- ✓ контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией;
- ✓ расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- ✓ разработку схемы организации криптографической защиты конфиденциальной информации (с указанием наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются, обладателей конфиденциальной информации, реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации, а также с указанием типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники). Указанную схему утверждает лицензиат ФАПСИ.

Приказ ФАПСИ от 13.06.2001 № 152

Инструкция 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

Инструкция определяет единый порядок защиты информации (не гос. тайны) средствами криптографической защиты на территории Российской Федерации.

Лицензиаты ФСБ России несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции.

- ✓ К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФСБ России допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.
- ✓ Лиц, оформляемых на работу в органы криптографической защиты, следует ознакомить с настоящей Инструкцией под расписку.
- ✓ Обязанности, возлагаемые на сотрудников органа криптографической защиты, могут выполняться штатными сотрудниками или сотрудниками других структурных подразделений, привлекаемыми к такой работе по совместительству.
- ✓ Сотрудники органа криптографической защиты должны иметь разработанные в соответствии с настоящей Инструкцией и утвержденные лицензиатом ФСБ России **функциональные обязанности**. Объем и порядок ознакомления сотрудников органов криптографической защиты с конфиденциальной информацией определяется обладателем конфиденциальной информации.

Функциональные обязанности по 152-й Инструкции

- Пользователи допускаются к работе с СКЗИ согласно перечню, утвержденного организацией и после прохождения соответствующего обучения;
 - Не разглашение конфиденциальной информации, к которой допущен пользователь, рубежи ее защиты, в том числе сведения о криптоключях;
 - Соблюдение требований к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
 - Уведомление ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
 - Сдача СКЗИ в соответствии с порядком, установленным Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
 - Немедленное уведомление ОКЗ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.
- Соблюдение режима конфиденциальности при обращении со сведениями, которые доверены АБ или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;
 - Точное выполнение требований к обеспечению безопасности конфиденциальной информации;
 - Надежное хранение СКЗИ эксплуатационной и технической документации к ним а также ключей ЭП;
 - Своевременное выявление попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;



функциональные обязанности Администраторов безопасности



Установка (инсталляция), наладка шифровальных (криптографических) средств

Проведение работ по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства

Уничтожение СКЗИ

Соблюдение режима конфиденциальности при обращении со сведениями, которые доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним

Точное выполнение требований к обеспечению безопасности конфиденциальной информации

Надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации

Своевременное выявление и информирование ОКЗ о попытках посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним

Немедленное уведомление ОКЗ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений

При увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать установленным порядком СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в ОКЗ

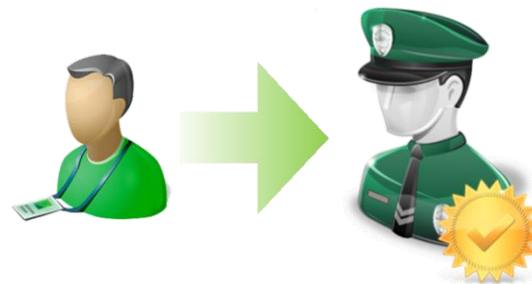
Допуск к работе

Обучение правилам
работы с СКЗИ

Сдача зачета по
программе
обучения

Утвердить перечень
лиц допущенных к
самостоятельной
работе с СКЗИ

Ознакомление с 152-
й инструкцией и
функциональными
обязанностями



Порядок эксплуатации СКЗИ

Эксплуатация СКЗИ должна проводиться в соответствии с эксплуатационной документацией, предусмотренной Формуляром, и в соответствии с разделом V "Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение-2005)"*

С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, обладатель, пользователь (потребитель) данной информации, установивший режим ее защиты с применением СКЗИ, а также собственник (владелец) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.



Порядок обеспечения информационной безопасности при использовании СКЗИ определяется руководителем эксплуатирующей организации на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ*

При эксплуатации СКЗИ необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К)*

При эксплуатации СКЗИ необходимо руководствоваться ПКЗ-2005**

* ЖТЯИ. 00087-01 91 01. КriptoПро CSP. Формуляр

** Положение ПКЗ-2005 "О разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации"

Требования по защите от НСД с использованием СКЗИ

Наряду с применением средств защиты от НСД необходимо выполнение организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

В организации, эксплуатирующей СКЗИ, должен быть назначен **администратор безопасности**, на которого возлагаются задачи проведения работ по использованию СКЗИ*

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку*

* ЖТЯИ.00087-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть

Услуги лицензируемых видов деятельности ОКЗ АО «Гринатом»

CLB.11

Услуга Корпоративного
удостоверяющего
центра

21. Передача шифровальных (криптографических) средств.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

CLB.18

Услуга Органа
криптографической
защиты

21. Передача шифровальных (криптографических) средств.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

GEN.23

Услуга Администратора
безопасности

12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.
13. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
21. Передача шифровальных (криптографических) средств.
24. Передача средств изготовления ключевых документов.
28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Услуги лицензируемого вида
деятельности ОКЗ АО «Гринатом»

CLB.11

Услуга Корпоративного
удостоверяющего центра

- ✓ Создание и выдача СКПЭП
- ✓ Приостановка и возобновление действия сертификатов
- ✓ Предоставление сервисов OSCP и TSP
- ✓ Изготовление списка отозванных сертификатов

CLB.18

Услуга Органа
криптографической защиты

- ✓ Передача дистрибутива и бесср. лицензии на СКЗИ
- ✓ Выдача заключений о возможности эксплуатации СКЗИ
- ✓ Разработка и ведение схемы криптозащиты
 - ✓ Проверка организации и обеспечения безопасности

GEN.23

Услуга Администратора
безопасности

- ✓ Обучение пользователей работе с СКЗИ
- ✓ Оформление экпл. Документации
- ✓ Установка СКЗИ на АРМ пользователя
- ✓ Контроль за соблюдением условий исп. СКЗИ

CLB.21

Услуга оценки уровня
доверия систем

- ✓ Выявление рисков ИБ при закл. договоров на эксплуатацию Систем
- ✓ Выдача заключения о возможности экпл. Систем
 - ✓ Контроль и приведение в соотв. Систем с требованиями ИБ
- ✓ Мониторинг норм.-правовой базы

Услуга CLB.18

Заявление на СКЗИ (с передачей СКЗИ)

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)

« 01 » января 20 15 г.

Закрытое акционерное общество «Институт ядерных исследований»

наименование организации, включая организационно-правовую форму

в лице

генерального директора

должность

Смирнова Бориса Петровича

фамилия, имя, отчество

действующего на основании

Устава

просит ОКЗ ЗАО «Гринатом»:

1. 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 «Отраслевыми требованиями по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014 в организации, расположенной по адресу:

600017, г. Владимир, ул. Горького, д. 5

Услуга CLB.18

Заявление на СКЗИ (с передачей СКЗИ)

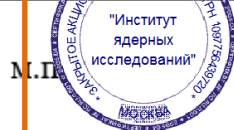
функции ОКЗ возлагаются на администраторов безопасности, назначенных Приказом № 427 от 01.01.2015. Копия Приказа прилагается.

№ п/п	Пользователь СКЗИ (должность, Ф.И.О.)	Вид защищаемой информации	Автоматизированная/информационная система	Учетный номер АРМ, на котором установлено СКЗИ	Подразделение	Адрес месторасположения АРМ	Общесистемное программное обеспечение, установленное на АРМ
1	Смирнов Борис Петрович, генеральный директор	Коммерческая тайна, персональные данные	ЗКПС	118	Администрация	600017, г. Владимир, ул. Горького, д. 5, каб. 214	Windows 7
2	Сидоров Дмитрий Иванович, бухгалтер	Коммерческая тайна, персональные данные	ИС РЦК	119	Отдел БУ и НУ	600017, г. Владимир, ул. Горького, д. 5, каб. 215	Windows 7
3	Васильев Александр Геннадьевич, главный специалист	Коммерческая тайна, персональные данные	SAP SRM	120	ИБ	600017, г. Владимир, ул. Горького, д. 5, каб. 216	Windows 7

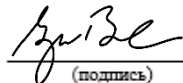
Администратор безопасности


/ И.И. ИВАНОВ /
(подпись) (ФИО)

Уполномоченное должностное лицо
генеральный директор



М.П.


/ Б.П. СМЕРНОВ /
(подпись) (ФИО)

Требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ*

На технических средствах, предназначенных для работы с СКЗИ должно использоваться только лицензионное ПО

На ПЭВМ не должны устанавливаться средства разработки ПО и отладчики.

Инсталляция СКЗИ должна производиться только с дистрибутива, полученного по доверенному каналу

При назначении паролей (для входа в ОС, BIOS) необходимо выполнение правил:

- ✓ длина пароля не менее 8 символов;
- ✓ Обязательно присутствие буквы в верхнем и нижнем регистрах включая спецсимволы;
- ✓ Пароль не должен включать в себя общепринятые сокращения (USER, ADMIN и т.д.);
- ✓ Новый пароль должен отличаться от старого не менее чем в 4-х позициях;
- ✓ Срок смены пароля не должен превышать 6 месяцев

Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время загрузки не проходят строенные тесты

Запретить сохранение паролей, используемых в работе с СКЗИ (пин-коды ключей и т.д.)
Включить групповую политику «Запретить использование сохраненных паролей»

СКЗИ должно использоваться с сертифицированными средствами антивирусной защиты

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены СКЗИ, вход согласно утвержденному перечню лиц



При эксплуатации СКЗИ ЗАПРЕЩАЕТСЯ:*

Вносить какие-либо изменения в программное обеспечение СКЗИ

Осуществлять несанкционированное ОКЗ 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

Записывать на ключевые носители постороннюю информацию

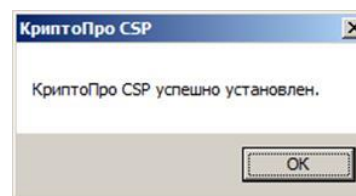
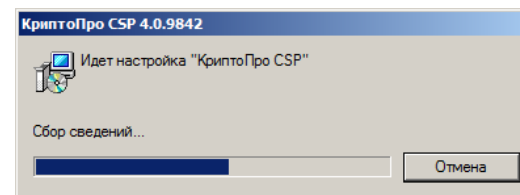
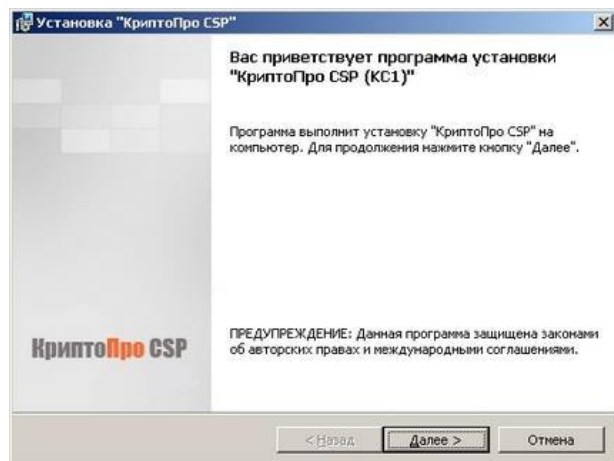
Осуществлять несанкционированное вскрытие ПЭВМ

Использовать нестандартные, измененные или отладочные версии ОС

Устанавливать несколько копий ОС

Установка СКЗИ «КриптоПро CSP» 4.0

Для установки СКЗИ требуется запустить файл-установщик соответствующий разрядности ОС. В ходе установки необходимо выбрать режим выборочной установки и установить ВСЕ компоненты.



GRINATOM

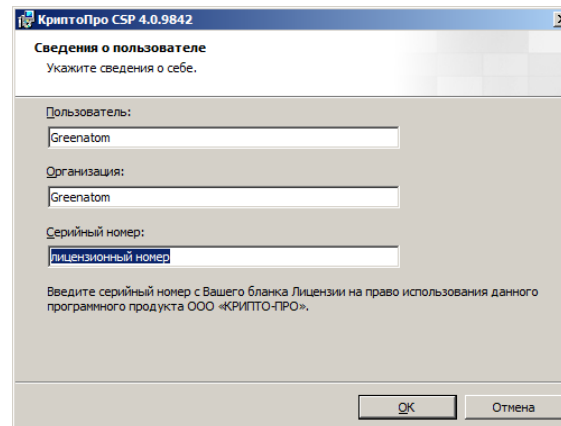
Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование службы хранения ключей. Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Ввод лицензии на СКЗИ «КриптоПро CSP» 4.0

По условиям лицензионного соглашения имеется ограничение срока использования «КриптоПро CSP 4.0», которое составляет 90 дней с момента непосредственной установки продукта

Лицензию на право использования продукта можно получить в ОКЗ.
Ввести серийный номер можно как при установке СКЗИ так и после.
Вкладка «Общие» > кнопка «Ввод лицензии», далее открывается окно, номер лицензии вносится поле «Серийный номер»



КриптоПро CSP 4.0.9842

Сведения о пользователе
Укажите сведения о себе.

Пользователь:
Greenatom

Организация:
Greenatom

Серийный номер:
лицензионный номер

Введите серийный номер с Вашего бланка Лицензии на право использования данного программного продукта ООО «КРИПТО-ПРО».

ОК Отмена

Удаление СКЗИ «КриптоПро CSP» 4.0

Рекомендуется сначала удалить установленные продукты через «Установку и удаление программ», перезагрузить компьютер, и затем запустить cspclean.exe.

Утилита предназначена для очистки компьютера от не удалённых элементов продуктов КРИПТО-ПРО. После завершения работы утилиты обязательно перезагрузите компьютер.

Ставим отметку об уничтожении в журнале поэкземплярного учета в строке с лицензией КриптоПро CSP. Столбец №12 заполняем дату удаления; №13 ФИО администратора безопасности; №14 подпись

Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов		
Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении
12	13	14

Ведение документации на СКЗИ

Журнал поэкземплярного учета СКЗИ – учет дистрибутива и документации

Формуляр и CD с дистрибутивом СКЗИ регистрируются в журнале поэкземплярного учета при получении. Администратор безопасности заполняет наименование, серийный номер, информацию от кого получено, указывает номер сопроводительного письма (если получено фельдъегерской связью), ФИО, дату получения, а также ставит свою подпись. Номера аппаратных средств при учете формуляра и материального носителя не указываются.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серийных 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. сотрудника в органе криптографической защиты, пользователей СКЗИ, производящих подключение (установку)	Дата подключения (подписи лиц, производящих подключение (установку))	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, производящих изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Формуляр «КриптоПро CSP» версия 4.0 RU	ЖТЭИ.00087-01 30 01		АО «Гринатом»	22-2-6-01/1111 01.01.2017	Фамилия И.О. Администратора безопасности	01.01.2017							Наименование предприятия
2	CD с дистрибутивом «КриптоПро CSP» версия 4.0 RU	385C1-1002699-001		АО «Гринатом»	22-2-6-01/1111 01.01.2017	Фамилия И.О. Администратора безопасности	01.01.2017							Наименование предприятия

Ведение документации на СКЗИ

Журнал поэкземплярного учета СКЗИ – учет установки у пользователя

Установка СКЗИ у пользователя тоже регистрируется в журнале. Администратор безопасности заполняет наименование СКЗИ (с полным указанием версии), в столбце серийные номера указывает номер дистрибутива (CD) с которого была произведена установка и номер лицензии, далее указывает информацию от кого получено, номер сопроводительного письма (если получено фельдъегерской связью), ФИО пользователя и дату установки, ФИО администратора с датой установки, далее номера аппаратных средств (серийный номер ПК) а также необходимо поставить подпись пользователю и администратору безопасности.

№ 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. сотрудника в органа криптографической защиты, пользователей СКЗИ, производивших подключение (установку)	Дата подключения (установки) подписи лиц, производивших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователей 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
	КриптоПро CSP 4.0 R2	Дистр. 385К-045112.001 Лицензия: 4040X-00000-12345- SX001-Z0006		АО «Гринатом»	22.2.6-01/1111 01.01.2017	Фамилия И.О. пользователя	01.01.2017	Фамилия И.О. Администратора безопасности	01.12.2016	Идентификационный или серийный номер АРМ				Наименование предприятия

Ведение документации на СКЗИ

Акт готовности СКЗИ к эксплуатации

В этом документе указываются наименование организации с фактическим адресом, наименования сертифицированных ФСТЭК антивирусных средств и средств защиты от НСД, номера помещений и рабочих мест, номера аппаратных средств, номера пломб, которыми опечатан ПК. Версия СКЗИ указывается полностью, например КриптоПро CSP 4.0 R2. В конце документа администратор ставит подпись.

Акт № _____
 готовности СКЗИ « КриптоПро CSP » версии 4.0 R2 к эксплуатации
(наименование СКЗИ)
 г. Москва « 28 » 06 20 17 г.

Администратор безопасности Иванов И.И. Ivanov@atom.ru
(Фамилия И.О., e-mail)
 составил настоящий акт в том, что произведена проверка готовности АРМ
 обладателя конфиденциальной информации
 ЗАО «Институт ядерных исследований»,
 г. Москва, ул. Строителей, д.22, стр.5
(Наименование организации, фактический адрес)

к эксплуатации СКЗИ на соответствие Отраслевым требованиям по
 информационной безопасности №1/910-П-дсп от 23.09.2014 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.

СКЗИ « КриптоПро CSP » версии 4.0 R2 установлено:

№ п/п	№ помещения и рабочего места	Уч.№ ПЭВМ	ПЭВМ опечатана печатью №	Операционная система
1	Каб. 22, рм №3	DIT_MC 0716_0178	08624693	Windows 7
2	Каб. 22, рм №1	DIT_MC 0716_0111	08624694	Windows 7

Вывод:

Оборудование АРМ соответствует Отраслевым требованиям по
 информационной безопасности №1/910-П-дсп от 23.09.2014 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 « КриптоПро CSP »
 версии 4.0 R2 .
(Наименование СКЗИ)

_____/ Иванов И.И.
(подпись) (Ф.И.О.)

Контроль	Выполнено/не выполнено, подпись
Установлено сертифицированное антивирусное ПО: <u>Kaspersky Endpoint Security 10</u> <small>(наименование продукта)</small>	выполнено _____ <small>(подпись)</small>
Установлено сертифицированное СЗИ от НСД: <u>SecretNet 7</u> <small>(наименование продукта)</small>	выполнено _____ <small>(подпись)</small>
ОС настроена в соответствии с отраслевыми требованиями по информационной безопасности №1/910-П-дсп от 23.09.2014	_____ <small>(подпись)</small>
Установлено СКЗИ в соответствии с документацией, поставляемой в комплекте. Проверено выполнение требований документа «Порядок разрешительного доступа пользователей и эксплуатирующего персонала к АРМ с установленным СКЗИ»	выполнено _____ <small>(подпись)</small>



Ведение документации на СКЗИ

Допуск пользователей и обучение – Заключение о сдаче зачетов

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения. Документом, подтверждающим должную специальную подготовку пользователей для самостоятельной работы с СКЗИ является заключение, составленное комиссией соответствующего ОКЗ на основании принятых от этих лиц зачетов по программе обучения.

Заключение составляется и подписывается администраторами безопасности комиссионно (минимум 2 человека) на основании ответов пользователей по анкете опроса - приложение №19 к Регламенту ОКЗ, учебные материалы для самостоятельного изучения направляются пользователю - приложение №18 к Регламенту ОКЗ.

Заключение о сдаче зачетов

№ п/п	Наименование организации	ФИО обучающегося	Зачтено/не зачтено
1	АО «Атом»	Бучко Игорь Юрьевич	Зачтено
2	АО «Атом»	Иванов Константин Семенович	Зачтено
3	АО «Атом»	Авдеев Николай Александрович	Зачтено

Состав проверяющей комиссии:

ФИО Администратора безопасности, должность, отдел, управление	Подпись, дата
Смирнов Александр Васильевич, Специалист, Отдел информационной безопасности	_____ / _____
Соболев Иван Андреевич, Начальник, Отдел информационной безопасности	_____ / _____

Аппаратный журнал

Приложение № 3 к 152-й Инструкции ФАПСИ

Аппаратный журнал ведет работник ОКЗ в случае если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией.

№ п.п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10
1	01.04.2017	КриптоПро CSP 4.0 R2 Номер лицензии	Установил ФИО Подпись	Rutoken	XXXX-XXXX-XXXX-XXXX	086123321			

Центр криптографической защиты

Вся необходимая информация и актуальные новости находятся на сайте Кripto Центра

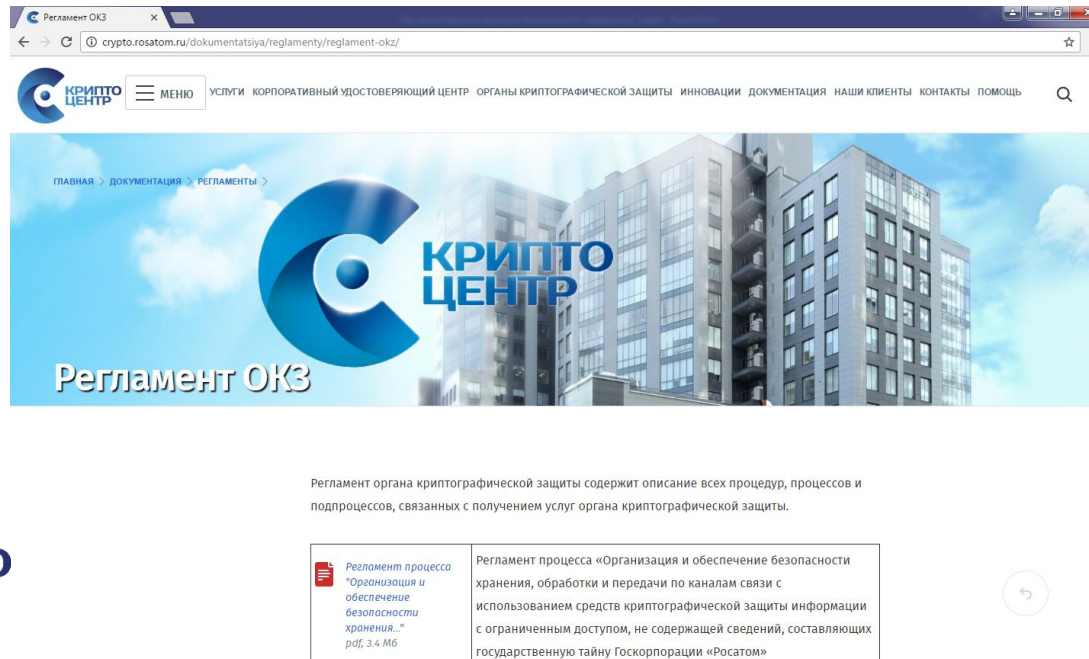
<http://crypto.rosatom.ru>

E-mail:

okz@greenatom.ru

Регламент ОКЗ АО «Гринатом», а также примеры заполнения документов расположены по ссылке:

<http://crypto.rosatom.ru/dokumentatsiya/reglamenti/reglament-okz/>



Услуга CLB.11

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи



Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

« 08 » апреля 2016 г.

Закрытое акционерное общество "Институт ядерных исследований"

наименование организации, включая организационно-правовую форму

в лице

Финансового директора

должность

Иванова Ивана Ивановича

фамилия, имя, отчество

действующего на основании

доверенности 20/3/2016-ДОВ от 01.02.2016

просит:

1. Создать квалифицированный сертификат ключа проверки электронной подписи (далее - сертификат) содержащий следующие данные:

Наименование	Длина	Значение
Общее имя	64	ЗАО "Институт ядерных исследований"
Организация	64	ЗАО "Институт ядерных исследований"
Адрес (ул., дом)	30	ул. Полянка, дом 24
Населённый пункт	128	город Москва
Регион	128	77 г. Москва
ИНН	12	007706712345
ОГРН	13	1097756439720
Страна	2	RU

Услуга CLB.11

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

2. Внести в сертификат данные владельца сертификата, полномочного представителя организации:

Наименование	Длина	Значение
Фамилия	40	Сидоров
Имя Отчество	64	Григорий Павлович
Должность	64	Специалист
Подразделение	64	Отдел безопасности
Email	128	GPSidorov@Greenatom.ru
СНИЛС	11	13431681234
Уч. запись в домене GK		GPSidorov @gk.rosatom.local

3. Указать область ограничения использования сертификата:

Квалифицированный сертификат Госкорпорации "Росатом"

4. Предоставить ключевой носитель и сертификат (отметить галочкой):

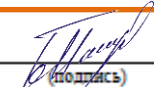
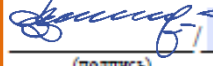
В Корпоративном удостоверяющем центре по адресу: г. Москва, ул. Большая Ордынка, д. 24, к. 481	<input checked="" type="checkbox"/>
Службой специальной связи по адресу (указать адрес и имя получателя):	<input type="checkbox"/>

Владелец сертификата соглашается с обработкой своих персональных данных ЗАО «Гринатом» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

Владелец сертификата ключа проверки электронной подписи

Уполномоченное должностное лицо
Финансовый директор
(Должность)



 (подпись)	Г.П. Сидоров (ф.ИО)
 (подпись)	И.И. Иванов (ф.ИО)

Услуга CLB.11

Доверенность пользователя Удостоверяющего центра

Доверенность пользователя Удостоверяющего центра

г. Москва

« 08 » апреля 2016 г.

Закрытое акционерное общество "Институт ядерных исследований"

наименование организации, включая организационно-правовую форму

в лице Финансового директора

(должность)

Иванова Ивана Ивановича

(фамилия, имя, отчество)

действующего на основании доверенности 20/3/2016-ДОВ от 01.02.2016

уполномочивает Сидорова Григория Павловича

(фамилия, имя, отчество)

4501 № 6654178, выдан ОВД района "Митино" города Москвы, 01.12.2002 г.

(серия и номер паспорта, кем и когда выдан)

1. Получить сертификат ключа проверки электронной подписи в Корпоративном удостоверяющем центре Госкорпорации «Росатом».

2. При использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Регламента Удостоверяющего центра по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра.

Услуга CLB.11

Доверенность пользователя Удостоверяющего центра

Настоящая доверенность действительна по < 12 > мая 2018 г.

Подпись пользователя Удостоверяющего центра
подтверждаю.

Г.П. Сидоров
фамилия, имя, отчество



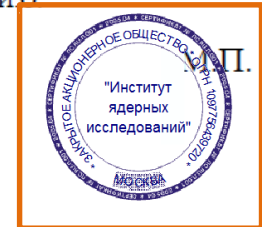
подпись

Уполномоченное должностное лицо
Финансовый директор
(должность)



подпись

И.И. Иванов
Ф.И.О.



* Примечание: срок действия доверенности должен быть не менее срока действия закрытого ключа, соответствующего создаваемому сертификату

Услуга CLB.11

Заявление на аннулирование сертификата

Приложение № 8

Заявление на аннулирование сертификата ключа проверки электронной подписи

«01» января 2016 г.

Закрытое акционерное общество «Институт ядерных исследований»

наименование организации, включая организационно-правовую форму

в лице Генерального директора

должность

Смирнова Бориса Петровича

фамилия, имя, отчество

действующего на основании Устава

Просит внести в реестр удостоверяющего центра информацию об аннулировании сертификата ключа проверки электронной подписи:

Серийный номер сертификата	2e1670ed00000000515d
Причина аннулирования сертификата	Увольнение

Услуга CLB.11

Заявление на аннулирование сертификата

Владелец сертификата ключа проверки электронной подписи



И.И. Иванов

(подпись)

(ФИО)

Уполномоченное должностное лицо

Генеральный директор



Б.П. Смирнов

(подпись)

(ФИО)

Отметки удостоверяющего центра

Отметка Оператора УЦ.

Данные, указанные в заявлении, проверены.

Сведения об аннулировании сертификата
ключа проверки электронной подписи занесены
в реестр УЦ

_____ / _____ /

«__» _____ 201__ г.

Ведение документации на СКЗИ



Учет ключевых документов

Ключи ЭП учитываются двумя строками, в первой строке указывается серийный номер сертифицированного носителя, во второй серийный номер сертификата (номер можно посмотреть на зеленой бумажке или же через КриптоПро CSP), номера аппаратных средств указывать не требуется.

№ 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. сотрудника в органа криптографической защиты, пользователей СКЗИ, производивших подключение (установку)	Дата подключения (подписи лиц, производивших подключение (установку))	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудника органа криптографической защиты, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Сертификат ключа проверки ЭП		252В 455В 0000 0000 561Е	АО «Гринатом»		Кипринова Ольга Владимировна	01.12.2016							Наименование предприятия
	Ключевой носитель Рутокен	0879774745		АО «Гринатом»		Кипринова Ольга Владимировна	01.12.2016							Наименование предприятия

Обязанности ОКЗ по контролю

Лицензиаты ФАПСИ обязаны контролировать выполнение обладателями конфиденциальной информации данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение такими обладателями условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией.

Органы криптографической защиты (координирующие органы криптографической защиты) должны обобщать результаты всех видов контроля, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок.

Обладатель конфиденциальной информации вправе обратиться в федеральные органы правительственной связи и информации с просьбой о проведении на договорной основе государственного контроля с целью оценки достаточности и обоснованности принимаемых лицензиатом ФАПСИ мер защиты его конфиденциальной информации.

Контроль ОКЗ АО «Гринатом»

В соответствии с Договором Присоединения №22/2143-Д на оказание услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств Орган криптографической защиты АО «Гринатом» проводит проверку организации и обеспечения безопасности информации с использованием средств криптографической защиты.

В ходе проверки изучаются и оцениваются:

- ✓ Администратор безопасности
 - ✓ Документы
 - ✓ Помещения и хранилища
- ✓ АРМ с установленными СКЗИ и Пользователи СКЗИ
- ✓ Сроки и периодичность проверок Органом криптографической защиты АО «Гринатом»: в соответствии с утвержденным Планом-графиком проверок.

Этапы проверки:

- ✓ Утверждается ОКЗ АО «Гринатом» программа проверки;
 - ✓ Проводится проверка;
- ✓ По результатам проверки составляется акт проверки, с которым ОКЗ АО «Гринатом» ознакомливает руководителя проверяемой организации;
 - ✓ Проверяемой стороной составляется План устранения недостатков;
- ✓ ОКЗ АО «Гринатом» контролирует выполнение Плана устранения недостатков.

Администратор безопасности в ходе проверки должен:

- ✓ Предоставлять проверяющим всю необходимую им информацию и всячески способствовать проведению проверки
 - ✓ Стараться устранить выявленные недостатки в ходе проверки

Контроль ФСБ России

Органы ФСБ наделены правом осуществлять государственный контроль за организацией и функционированием криптографической безопасности информационно-телекоммуникационных систем, сетей связи, обеспечивающих передачу информации с использованием шифров.

Согласно разделу V Инструкции, утв. Приказом ФАПСИ от 13.06.2001г №152 в ходе государственного контроля изучаются и оцениваются:

- ✓ организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- ✓ достигнутый уровень криптографической защиты конфиденциальной информации;
- ✓ условия использования СКЗИ.

Сроки и периодичность государственного контроля определяет ФСБ России.



Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности». Ст.11.2.

Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности». Ст.12, п. И.1.

Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности». Ст.13, п. Щ.

«Положение о Федеральной службе безопасности Российской Федерации», утвержденное Указом Президента РФ от 11.08.2003 № 960. Ст.9

Ответственность

Ответственность пользователя за разглашение коммерческой тайны

Трудовой кодекс РФ

ст.81 ТК РФ
Расторжение трудового договора по инициативе работодателя

Кодекс РФ об административных правонарушениях

ст.13.14 КОАП РФ
Наложение адм. штрафа от **500** до **1000 руб.** (на граждан) и от **4000** до **5000 руб.** (на должностных лиц)

Уголовный кодекс РФ

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

ст.13.11-14 КОАП РФ
Штраф до **30 000 руб.** с конфискацией, приостановление деятельности организации на срок до **90 суток**

Уголовный кодекс РФ

ст.137, 138, 171, 183, 272, 273, 274, 293 УК РФ
Наказание до 7 лет лишения свободы штраф до **1 млн. руб.**

**Развитие услуг
лицензируемых
видов деятельности
АО «Гринатом»**

- Предприятия**
- Услуга Корпоративного удостоверяющего центра**
(Кол-во выданных сертификатов электронной подписи)
- Услуга органа криптографической защиты**
(Средства криптографической защиты информации и администраторы безопасности)
- Услуга Администратора Безопасности**
(Количество автоматизированных рабочих мест на обслуживании)
- Услуга оценки и контроля уровня доверия систем к требованиям ГК «Росатом»**

2012



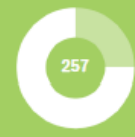
1128



556

97

2013



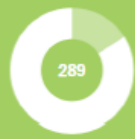
4102



3285

185

2014



4917



4116

118



89

2015



7573



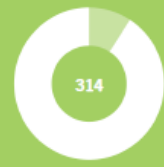
6249

130



818

2016



9014



7037

179



2663

