

Типовой регламент
проведения в пределах полномочий мероприятий по контролю (надзору) за
выполнением требований, установленных Правительством Российской Федерации, к
обеспечению безопасности персональных данных при их обработке в информационных
системах персональных данных
(утв. ФСБ РФ 8 августа 2009 г. N 149/7/2/6-1173)

I. Общие положения.

1.1. Порядок организации и проведения проверки

1.1.1. Мероприятие по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - проверка) проводится на основании распоряжения или приказа начальника 8 Центра ФСБ России либо лица его замещающего. Проверка может проводиться только должностным лицом или должностными лицами, уполномоченными на проведение проверки, которые указаны в распоряжении или приказе начальника 8 Центра ФСБ России либо лица его замещающего.

1.1.2. В распоряжении или приказе начальника 8 Центра ФСБ России либо лица его замещающего указываются:

- 1) наименование органа государственного контроля (надзора);
- 2) фамилии, имена, отчества, должности должностного лица или должностных лиц, уполномоченных на проведение проверки, а также привлекаемых к проведению проверки экспертов, представителей экспертных организаций;
- 3) наименование юридического лица или фамилия, имя, отчество индивидуального предпринимателя, проверка которых проводится;
- 4) цели, задачи и предмет проверки;
- 5) правовые основания проведения проверки;
- 6) перечень мероприятий по контролю (надзору), необходимых для достижения целей и задач проведения проверки;
- 7) даты начала и окончания проведения проверки.

1.1.3. Заверенные печатью копии распоряжения или приказа начальника 8 Центра ФСБ России либо лица его замещающего вручаются под роспись должностными лицами 8 Центра ФСБ России, проводящими проверку, руководителю или уполномоченному представителю юридического лица, индивидуальному предпринимателю, его уполномоченному представителю одновременно с предъявлением служебных удостоверений.

1.1.4. По просьбе руководителя или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя должностные лица 8 Центра ФСБ России обязаны ознакомить подлежащих проверке лиц с настоящим документом.

1.1.5. Общий срок проведения проверки не может превышать двадцати рабочих дней.

1.1.6. В отношении одного субъекта малого предпринимательства общий срок проведения проверки не может превышать пятьдесят часов для малого предприятия, пятнадцать часов для микропредприятия в год.

1.2. Ограничения при проведении проверки

1.2.1. При проведении проверки должностные лица 8 Центра ФСБ России не вправе:

1) проверять выполнение требований, не относящихся к компетенции ФСБ России;

2) осуществлять плановую или внеплановую проверку в случае отсутствия при ее проведении руководителя или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя;

3) требовать представления документов, информации, если они не являются объектами проверки и не относятся к предмету проверки, а также изымать оригиналы документов, относящихся к предмету проверки;

4) распространять информацию, составляющую охраняемую законом тайну и полученную в результате проведения проверок, за исключением случаев, предусмотренных законодательством Российской Федерации;

5) превышать установленные сроки проведения проверки;

6) осуществлять выдачу юридическим лицам, индивидуальным предпринимателям предписаний или предложений о проведении за их счет мероприятий по контролю.

II. Программа

проведения работ по контролю (надзору) за использованием шифровальных (криптографических) средств, применяемых для обеспечения безопасности персональных данных в информационных системах персональных данных

N п/п	Проверяемые требования	Перечень представляемых документов и справок	Нормативные правовые акты, требования которых подлежат проверке
1	<p>Организация системы организационных мер защиты персональных данных:</p> <ul style="list-style-type: none"> - область применения средств криптографической защиты информации (далее - СКЗИ) в информационных системах персональных данных; - наличие ведомственных документов и приказов по организации криптографической защиты информации; - выполнение рекомендаций и указаний ФСБ России (при их наличии) по вопросам организации связи с использованием криптосредств. 	<p>Ведомственные документы и приказы по организации криптографической защиты информации.</p>	<p>Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных";</p> <p>Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";</p> <p>Постановление Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";</p> <p>Постановление Правительства РФ от 29 декабря 2007 г. N 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";</p> <p>Приказ ФСБ России от 9 февраля</p>
2	<p>Организация системы криптографических мер защиты информации:</p> <ul style="list-style-type: none"> - наличие модели угроз нарушителя; - соответствие модели угроз исходным данным; - соответствие требуемого уровня криптографической защиты полученной модели нарушителя; - соответствие используемых СКЗИ 	<p>Модель угроз, разработанная оператором.</p> <p>Документы по поставке СКЗИ оператору.</p>	<p>Постановление Правительства РФ от 29 декабря 2007 г. N 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";</p> <p>Приказ ФСБ России от 9 февраля</p>

	<p>полученному уровню криптографической защиты;</p> <ul style="list-style-type: none"> - наличие документов по поставке СКЗИ оператору. 		<p>2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), (зарегистрировано в Минюсте РФ 3 марта 2005 г., N 6382);</p> <p>Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, N 149/54-144, 2008 г.;</p> <p>Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, N 149/6/6-622, 2008 г.</p>
3	<p>Разрешительная и эксплуатационная документация:</p> <ul style="list-style-type: none"> - наличие необходимых лицензий для использования СКЗИ в информационных системах персональных данных; - наличие сертификатов соответствия на используемые СКЗИ; - наличие эксплуатационной документации на СКЗИ (формуляров, правил работы, руководств оператора и т.п.); - порядок учета СКЗИ, эксплуатационной и технической документации к ним; - выявление несертифицированных ФСБ России (ФАПСИ) СКЗИ. 	<p>Лицензии и сертификаты на используемые СКЗИ.</p> <p>Эксплуатационная документация на СКЗИ.</p>	
4	<p>Требования к обслуживающему персоналу:</p> <ul style="list-style-type: none"> - порядок учета лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационной системе; - наличие функциональных обязанностей ответственных пользователей СКЗИ; - укомплектованность штатных 	<p>Утвержденные список лиц, допущенных к работе с СКЗИ.</p> <p>Документы, подтверждающие функциональные обязанности сотрудников.</p> <p>Журнал учета пользователей криптосредств.</p> <p>Документы, подтверждающие прохождение обучения сотрудников.</p>	

	<p>должностей личным составом, а также достаточность имеющегося личного состава для решения задач по организации криптографической защиты информации;</p> <p>- организация процесса обучения лиц, использующих СКЗИ, применяемых в информационных системах, правилам работы с ними и другим нормативным документам по организации работ (связи) с использованием СКЗИ.</p>	
5	<p>Эксплуатация СКЗИ:</p> <p>- проверка правильности ввода СКЗИ в эксплуатацию и соответствие условий эксплуатации технических средств удостоверяющего центра (при наличии) требованиям эксплуатационной документации и сертификатов соответствия;</p> <p>- оценка технического состояния СКЗИ, соблюдения сроков и полноты проведения технического обслуживания, а также проверка соблюдения правил пользования СКЗИ и порядка обращения с ключевыми документами к ним.</p>	<p>Акты ввода СКЗИ в эксплуатацию. Журнал поэкземплярного учета СКЗИ. Журнал учета и выдачи носителей с ключевой информацией.</p>
6	<p>Оценка соответствия применяемых СКЗИ:</p> <p>- соответствие программного обеспечения, реализующего криптографические алгоритмы используемых СКЗИ, эталонным</p>	<p>Средства СКЗИ. Программное обеспечение СКЗИ (дистрибутив).</p>

	<p>версиям, прошедших сертификацию в ФСБ России;</p> <ul style="list-style-type: none">- проведение (при необходимости) на местах осуществления проверки оперативных тематических исследований используемых СКЗИ.	
7	<p>Организационные меры:</p> <ul style="list-style-type: none">- выполнения требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, а также соответствия режима хранения СКЗИ и ключевой документации предъявляемым требованиям;- оценка степени обеспечения оператора криптоключами и организации их доставки.- проверка наличия инструкции по восстановлению связи в случае компрометации действующих ключей к СКЗИ.- порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей персональных данных или использования СКЗИ.	<p>Эксплуатационная документация на СКЗИ.</p> <p>Помещения выделенные для установки СКЗИ и хранения ключевых документов к ним.</p> <p>Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ.</p>

При проведении проверки должностные лица 8 Центра ФСБ России вправе допускаться к СКЗИ, техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены СКЗИ, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных, и ключевых документов.

III. Порядок оформления результатов проверки

3.1. По результатам проверки должностными лицами 8 Цента ФСБ России, проводящими проверку, составляется акт в двух экземплярах.

3.2. В акте проверки указываются:

- 1) дата, время и место составления акта;
- 2) дата и номер распоряжения или приказа, на основании которого проведена проверка;
- 3) фамилия, имя, отчество и должности должностного лица или должностных лиц, проводивших проверку;
- 4) объект проверки, а также фамилии, имена, отчества операторов (ответственных пользователей криптосредств), осуществляющих обработку персональных данных, в отношении которых проводится проверка;
- 5) сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований, об их характере, о лицах, на которых возлагается ответственность за совершение этих нарушений;
- 6) сведения об ознакомлении или об отказе в ознакомлении с актом оператора, осуществляющего обработку персональных данных, а также лиц, присутствовавших при проведении проверки;
- 7) дата, время и место проведения проверки;
- 8) подписи должностного лица или должностных лиц, проводивших проверку.

3.3. К акту проверки могут прилагаться протоколы (заключения) проведённых экспертиз, объяснения должностных лиц, работников, на которых возлагается ответственность за нарушения обязательных требований, и другие документы или их копии, связанные с результатами проверки.

3.4. Акт оформляется непосредственно после завершения проверки в двух экземплярах, один из которых с копиями приложений, вручается оператору, осуществляющему обработку персональных данных, или уполномоченному им лицу под расписку об ознакомлении или отказе в ознакомлении с актом проверки.

3.5. В журнале учёта проверок должностными лицами 8 Центра ФСБ России осуществляется запись о проведённой проверке, содержащая сведения о датах начала и окончания проведения проверки, времени её проведения, правовых основаниях, целях, задачах и предмете проверки, выявленных нарушениях и выданных предписаниях, а также указываются фамилии, имена, отчества и должности должностного лица или должностных лиц, проводящих проверку, его или их подписи (При отсутствии журнала учёта проверок в акте проверки делается соответствующая запись).

3.6. Юридическое лицо, индивидуальный предприниматель, проверка которых проводилась, в случае несогласия с фактами, изложенными в акте проверки, а также с выводами и предложениями проверяющих в течение 15 дней со дня получения акта проверки вправе представить письменные возражения по указанному акту в целом или по его отдельным положениям.

