ВВОД СЗ В ДЕЙСТВИЕ

ЭТАПЫ СОЗДАНИЯ СИСТЕМЫ ЗИ ГИС

п.13 Приказа ФСТЭК России №17

1. формирование требований к защите информации, содержащейся в информационной системе;
2. разработка системы защиты информации информационной системы;
3. **внедрение системы защиты информации информационной системы;**
4. аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
5. обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
6. обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

ЭТАПЫ


Определение имеющихся систем
Классификация ИС
Модель угроз и нарушителя безопасности, техническое задание на СЗ
Проект на систему защиты (+рабочая документация)
Покупка, установка СЗИ (СЗИ от НСД, антивирус, СОВ, криптошлюз с МЭ)
Разработка и утверждение ОРД
Приемо-сдаточные испытания СЗ
Аттестация ИС по требованиям безопасности

СОЗДАНИЕ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

ПП РФ №676

ГОСТ 51583-2014

Приказ ФСТЭК №17

ГОСТ 34.601-90

ГОСТ 34.603-92

ГОСТ РО 0043-003-2012

ГОСТ РО 0043-004-2013

3. Внедрение системы ЗИ АСЗИ

- Ввод в действие
- Аттестация АСЗИ

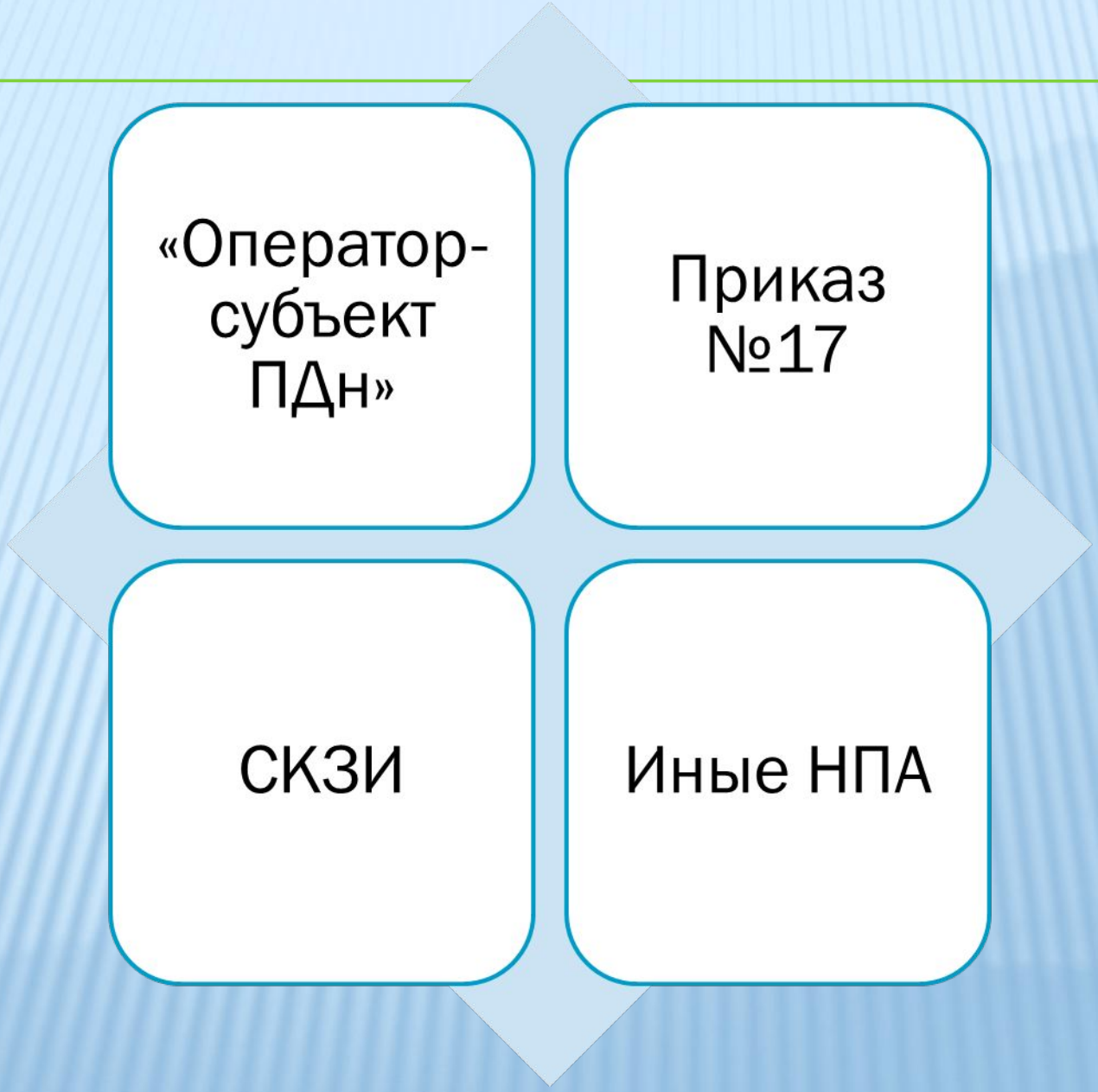
организуется заказчиком

проводится разработчиком

- установка и настройка СЗИ
- разработка и внедрение организационных мер ЗИ
- испытания

аттестацию АСЗИ на соответствие требованиям по ИБ

ОРД



организационно-распорядительные документы определяют правила и процедуры (Приказ № 17)

управления (администрирования) **системой защиты** информации информационной системы

выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации , и реагирования на них

управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы

контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе

защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

Управление системой защиты

заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе

управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей

установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению

Управление системой защиты

- централизованное управление системой защиты информации информационной системы (при необходимости)
- регистрация и анализ событий безопасности
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение
- сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации

Выявление инцидентов и реагирование на них

определение лиц, ответственных за выявление инцидентов и реагирование на них

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов

своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами

Выявление инцидентов и реагирование на них

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов

планирование и принятие мер по предотвращению повторного возникновения инцидентов

Управление конфигурацией

поддержание конфигурации информационной системы и ее системы защиты информации в соответствии с эксплуатационной документацией на систему защиты информации

определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации

Управление конфигурацией

управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе

- определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации,
- санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации,
- документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации,
- сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации,
- контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации

Управление конфигурацией

анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы

определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и ее системы защиты информации

внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации ИС

принятие решения по результатам управления конфигурацией о повторной аттестации ИС или проведении дополнительных аттестационных испытаний

ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ

Контроль за обеспечением уровня ЗИ

контроль за событиями безопасности и действиями пользователей в ИС

контроль (анализ) защищенности информации, содержащейся в ИС

анализ и оценка функционирования системы защиты информации ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы

периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации

документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС

принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС, повторной аттестации ИС или проведении дополнительных аттестационных испытаний

МЕРЫ ПО ЗИ В ИС

Приказ № 21	Приказ № 17
идентификация и аутентификация субъектов доступа и объектов доступа (6)	идентификация и аутентификация субъектов доступа и объектов доступа (7)
управление доступом субъектов доступа к объектам доступа (17)	управление доступом субъектов доступа к объектам доступа (17)
ограничение программной среды (4)	ограничение программной среды (4)
защита машинных носителей ПДн (8)	защита машинных носителей информации (8)
регистрация событий безопасности (7)	регистрация событий безопасности (8)
антивирусная защита (2)	антивирусная защита (2)
обнаружение (предотвращение) вторжений (2)	обнаружение (предотвращение) вторжений (2)
контроль (анализ) защищенности ПДн (5)	контроль (анализ) защищенности информации (5)
обеспечение целостности ИС и ПДн (8)	целостность ИС и информации (8)
обеспечение доступности ПДн (5)	доступность информации (7)
защита среды виртуализации (10)	защита среды виртуализации (10)
защита технических средств (5)	защита технических средств (5)
защита ИС, ее средств, систем связи и передачи данных (20)	защита ИС, ее средств, систем связи и передачи данных (30)
выявление инцидентов (6)	-
управление конфигурацией ИС и системы защиты ПДн (4)	-

НПА

ФЗ от 27.07.2006 № 152 «О персональных данных»

ПП РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПП РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПП РФ от 6 июля 2015 г. N 676 г. Москва «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных информации»

приказ ФСБ России от 10.09.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из УЗ»;

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 (утверждена приказом ФАПСИ № 152 от 13.06.2001).

НПА

ФЗ от 27.07.2006 № 152 «О персональных данных»

ПП РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПП РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПП РФ от 6 июля 2015 г. N 676 г. Москва «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных информации»

приказ ФСБ России от 10.09.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из УЗ»;

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 ПДн при их обработке в ИСПДн (утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622);

ФЗ от 27.07.2006 № 152 «О персональных данных» (ст.18.1)

1) **назначение оператором ответственного за организацию обработки ПДн;**

2) издание оператором **документов, определяющих политику оператора в отношении обработки ПДн**, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн настоящему ФЗ и принятым в соответствии с ним НПА, а также локальным актам оператора;

5) **оценка вреда**, который может быть причинен субъектам ПДн в случае нарушения ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ;

6) **ознакомление работников оператора** с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

ФЗ от 27.07.2006 № 152 «О персональных данных»

Согласие на обработку

1) ФИО, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) ФИО, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;

3) наименование или ФИО и адрес оператора, получающего согласие субъекта ПДн;

4) цель обработки ПДн;

5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;

6) наименование или ФИО и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено ФЗ;

9) подпись субъекта ПДн.

ФЗ от 27.07.2006 № 152 «О персональных данных»

Согласие на обработку

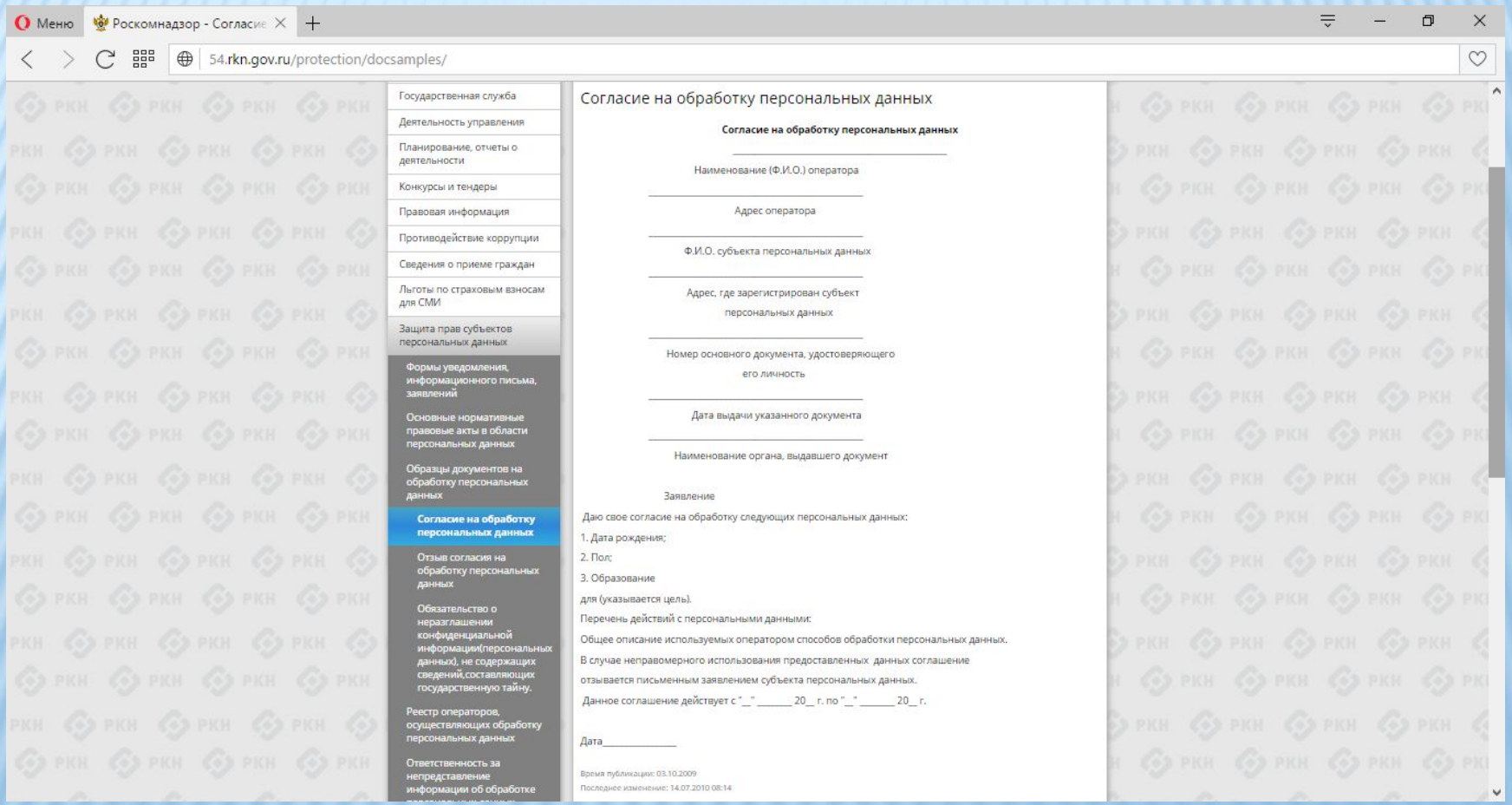
Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

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

(ФЗ № 63 «Об электронной подписи»)

ФЗ от 27.07.2006 № 152 «О персональных данных»

Согласие на обработку



ФЗ от 27.07.2006 № 152 «О персональных данных», ст. 16

3. Оператор обязан разъяснить субъекту персональных данных **порядок принятия решения** на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также **разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов**.

ФЗ от 27.07.2006 № 152 «О персональных данных», ст. 14

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

ФЗ от 27.07.2006 № 152 «О персональных данных», ст. 20

Оператор обязан предоставить **безвозмездно** субъекту персональных данных или его представителю **возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных**. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор **обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и** принять разумные меры ьих лиц, которым персональные данные э реданы.

ФЗ от 27.07.2006 № 152 «О персональных данных», ст. 21

В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. **Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя**, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

УВЕДОМЛЕНИЕ НЕ НУЖНО

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект ПДн;

3) относящихся к членам (участникам) общественного объединения или религиозной организации;

4) сделанных субъектом ПДн общедоступными;

5) включающих в себя только ФИО субъектов ПДн;

6) необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в ИСПДн, имеющие в соответствии с федеральными законами **статус государственных автоматизированных информационных систем**

8) обрабатываемых без использования средств автоматизации в соответствии ФЗ или иными НПА РФ, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн;

9) обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности,

УВЕДОМЛЕНИЕ

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

УВЕДОМЛЕНИЕ

7) описание мер, предусмотренных статьями 18.1 и 19 ФЗ №152, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

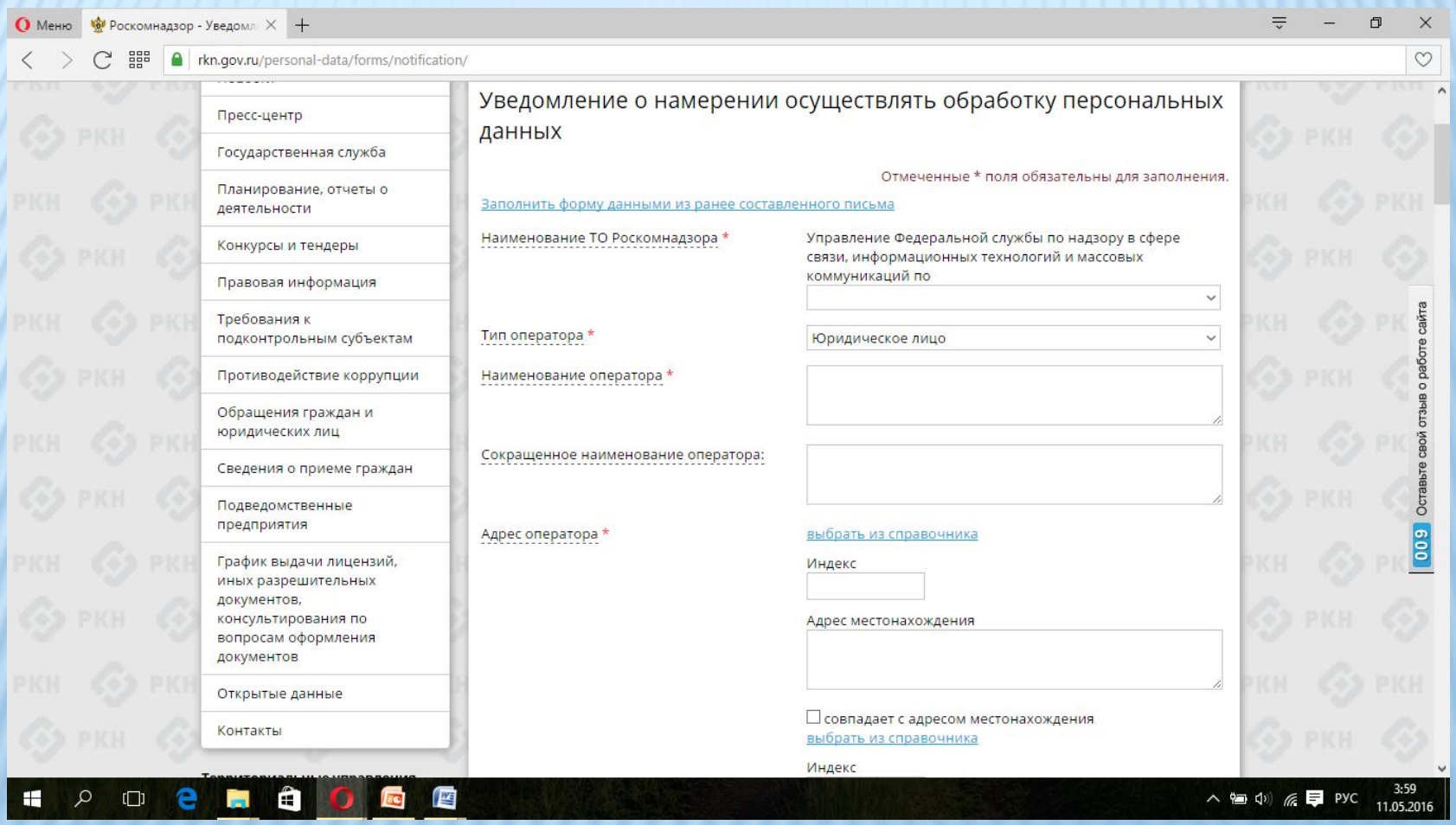
9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

УВЕДОМЛЕНИЕ



ПП РФ от 01.11.2012 № 1119

№ п/п	Формулировка требований	Уровень защищенности персональных данных			
		4	3	2	1
1.	Организация режима обеспечения безопасности помещений, в которых размещена ИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
2.	Обеспечение *сохранности носителей персональных данных*	+	+	+	+
3.	**Утверждение оператором документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения служебных обязанностей**	+	+	+	+
4.	Использование средств ЗИ, прошедших процедуру оценки соответствия, в случае, когда применение таких средств необходимо для нейтрализации угроз безопасности	+	+	+	+
5.	**Назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн при их обработке в ИС**	–	+	+	+
6.	Доступ к содержанию **электронного журнала сообщений**	-	-	+	+
7.	Автоматическая регистрация в электронном журнале безопасности изменения полномочий администратора	–	–	–	+
8.	Создание структурного подразделения, ответственного за обеспечение безопасности ПДн	–	–	–	+

ПП РФ от 15 сентября 2008 г. N 687

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

- а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
- в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

ПП РФ от 15 сентября 2008 г. N 687

2. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

- а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

ПП РФ от 15 сентября 2008 г. N 687

3. Меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить **места хранения персональных данных (материальных носителей)** и установить **перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.**

ПП ОТ 21 МАРТА 2012 Г. N 211 Г.

правила обработки персональных данных,

правила рассмотрения запросов субъектов персональных данных или их представителей;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

правила работы с обезличенными данными;

перечень информационных систем персональных данных;

перечни персональных данных

ПП ОТ 21 МАРТА 2012 Г. N 211 Г.

перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к персональным данным;

должностная инструкция ответственного за организацию обработки ПДн в государственном или муниципальном органе;

типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним государственного или муниципального контракта прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей;

типовая форма согласия на обработку ПДн служащих государственного или муниципального органа, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн;

порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка ПДн;

ПРИКАЗ ФСБ РФ ОТ 10 ИЮЛЯ 2014 Г. №378

Для уз-4 и выше

- б) утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- в) утверждения перечня лиц, имеющих право доступа в помещения.
- б) осуществлять поэкземплярный учет машинных носителей ПДн, который достигается путем ведения журнала учета носителей ПДн с использованием регистрационных (заводских) номеров.

ПРИКАЗ ФСБ РФ ОТ 10 ИЮЛЯ 2014 Г. №378

Для уз-4 и выше

- а) разработать и утвердить документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей;
- б) поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей.

ПРИКАЗ ФАПСИ № 152

- проверка готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ;

- обучение лиц, использующих СКЗИ, правилам работы с ними (осуществляет орган ОКЗ);

- 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;

ПЕРЕЧЕНЬ ОРД ПО СКЗИ

- Акт готовности к эксплуатации СКЗИ
- Заключение о допуске пользователя к СКЗИ
- Заключение о возможности к эксплуатации СКЗИ
- Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации

ПЕРЕЧЕНЬ ОРД ПО СКЗИ

- Перечень сотрудников, допущенных к работе с СКЗИ
- Приказ о назначении ответственного пользователя СКЗИ
- Инструкция ответственного пользователя
- Журнал учёта СКЗИ
- Форма акта уничтожения СКЗИ
- Перечень хранилищ для СКЗИ
- Акт ввода в эксплуатацию СКЗИ

ЭТАПЫ ВВОДА В ДЕЙСТВИЕ

Внедрение организационных мер защиты (Приказ №17)

реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения

проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации

отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации

ПРАКТИЧЕСКАЯ РАБОТА №4

- Заполнить журналы (по две-три записи в каждом)

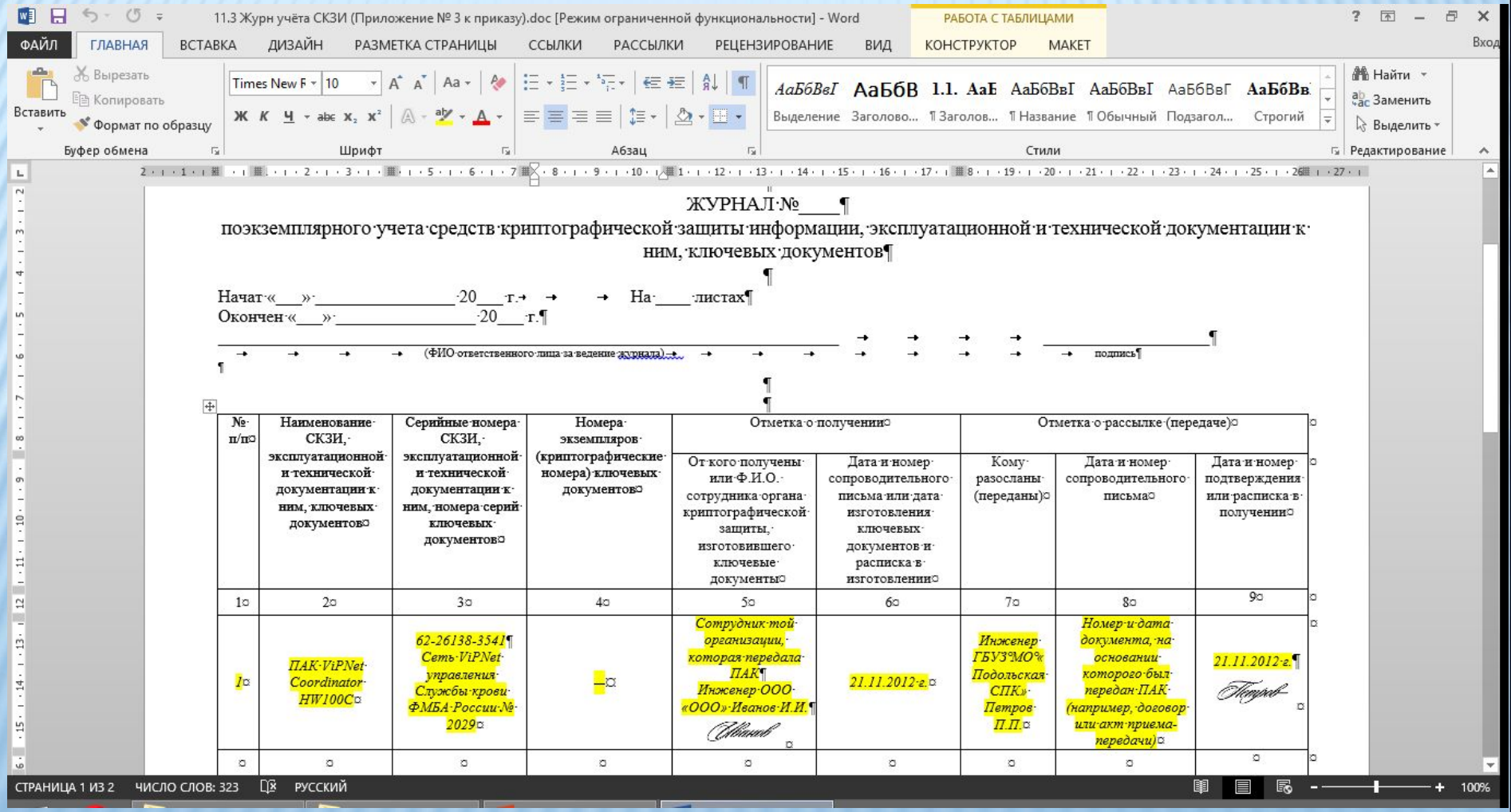
ТЕМЫ ОБУЧЕНИЯ

- Положения законодательства Российской Федерации в области защиты информации ограниченного доступа
- Требования нормативных документов ФСТЭК и ФСБ России в области защиты информации ограниченного доступа
- Требования ОРД Организации, регламентирующей вопросы обработки и защиты информации ограниченного доступа
- Меры защиты информации ограниченного доступа, применяемые в Организации
- Правила работы со средствами защиты информации (в том числе криптографическими)
- Деятельность сотрудников Организации для защиты

ВНУТРЕННИЙ КОНТРОЛЬ

- Проверка ведения журнала учёта машинных носителей информации
- Проверка расположения средств отображения информации
- Проверка ведения журналов событий безопасности
- Контроль состава технических средств, программного обеспечения и средств защиты информации
- Контроль установки обновлений программного обеспечения
- Проверка управления идентификаторами и средствами аутентификации

ЖУРНАЛ УЧЕТА СКЗИ



11.3 Журн учёта СКЗИ (Приложение № 3 к приказу).doc [Режим ограниченной функциональности] - Word

ЖУРНАЛ №____

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Начат «___» _____ 20___ г. На ____ листах

Окончен «___» _____ 20___ г.

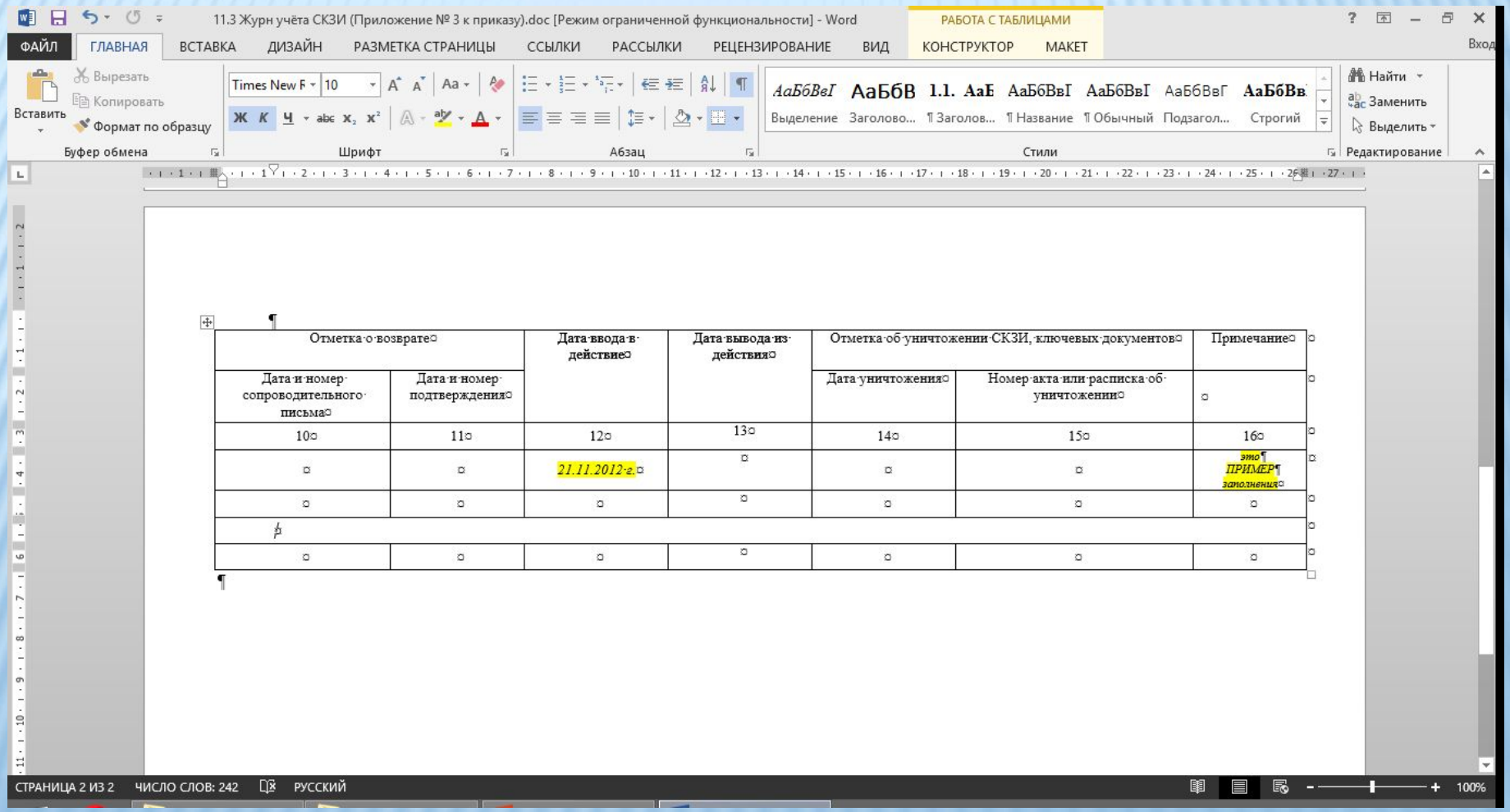
_____ _____

(ФИО ответственного лица за ведение журнала) подпись

№ 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)		
				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
1	2	3	4	5	6	7	8	9
1	ПАК ViPNet Coordinator HW100C	62-26138-3541 Сеть ViPNet управления Службы крови ФМБА России № 2029	–	Сотрудник той организации, которая передала ПАК Инженер ООО «ООО» Иванов И.И.	21.11.2012 г.	Инженер ГБУЗ МО "Подольская СПК" Петров П.П.	Номер и дата документа, на основании которого был передан ПАК (например, договор или акт приема-передачи)	21.11.2012 г.

СТРАНИЦА 1 ИЗ 2 ЧИСЛО СЛОВ: 323 РУССКИЙ 100%

ЖУРНАЛ УЧЕТА СКЗИ



11.3 Журн учёта СКЗИ (Приложение № 3 к приказу).doc [Режим ограниченной функциональности] - Word

РАБОТА С ТАБЛИЦАМИ

ФАЙЛ | ГЛАВНАЯ | ВСТАВКА | ДИЗАЙН | РАЗМЕТКА СТРАНИЦЫ | ССЫЛКИ | РАССЫЛКИ | РЕЦЕНЗИРОВАНИЕ | ВИД | КОНСТРУКТОР | МАКЕТ

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16
		21.11.2012 г.				это ПРИМЕР заполнения

СТРАНИЦА 2 ИЗ 2 | ЧИСЛО СЛОВ: 242 | РУССКИЙ | 100%

ВВОД СЗ В ДЕЙСТВИЕ

СПАСИБО ЗА ВНИМАНИЕ!