



Модуль 2

Организация обеспечения безопасности персональных данных в информационных системах персональных данных

Тема 2.1. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Особенности неавтоматизированной обработки персональных данных

ч. 3 ст. 19 152-ФЗ

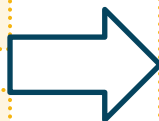
Правительство РФ с учетом:

- возможного вреда субъекту ПДн,
- объема и содержания ПДн,
- вида деятельности, при котором обрабатываются ПДн,
- актуальности угроз безопасности ПДн,

устанавливает:

1. Уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных.

2. Требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн.



Постановление Правительства
Российской Федерации
№ 1119
«Об утверждении требований к
защите персональных данных
при их обработке в
информационных системах
персональных данных»
(ПП 1119)

Основные положения ПП 1119

Документ устанавливает требования к защите персональных данных при их обработке в ИСПДн и уровни защищенности ПДн.

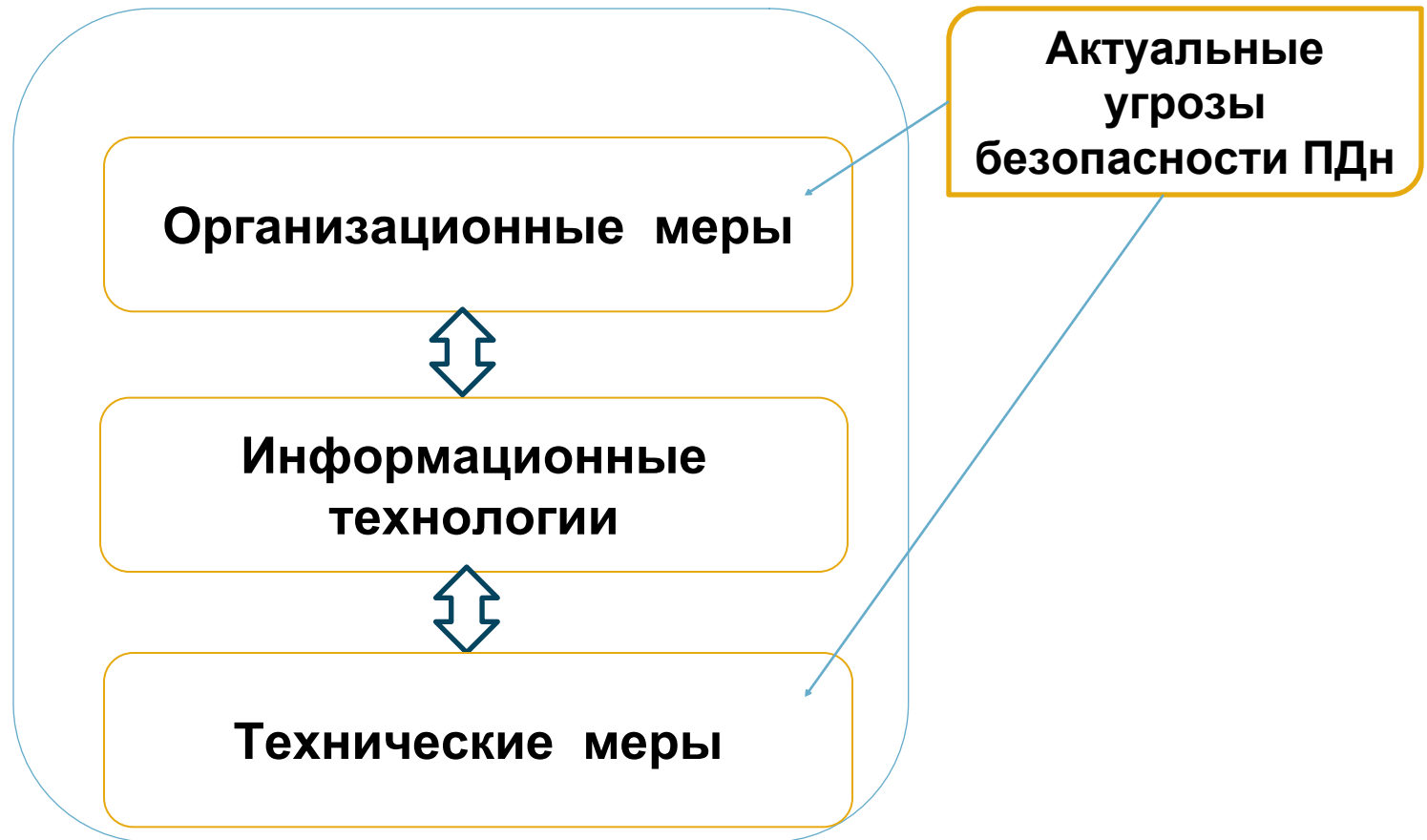


Безопасность персональных данных обеспечивается с помощью **системы защиты персональных данных**, нейтрализующей **актуальные** угрозы, определенные в соответствии с частью 5 статьи 19 ФЗ «О персональных данных».



Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом **актуальных** угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

Основные положения ПП 1119



Система защиты ПДн

Безопасность персональных данных

- Безопасность персональных данных при их обработке в ИСПДн обеспечивает **оператор этой системы** или **лицо, осуществляющее обработку** ПДн по поручению оператора (уполномоченное лицо) на основании заключаемого с этим лицом договора.
- Договор должен предусматривать обязанность уполномоченного лица обеспечить **безопасность** персональных данных при их обработке в ИСПДн.
- Выбор средств защиты информации для СЗПДн осуществляет **оператор** в соответствии с нормативными правовыми актами, принятыми ФСБ России и ФСТЭК России во исполнение ч.4. ст.19 ФЗ «О персональных данных».

Определение типов ПДн

Специальные категории персональных данных

персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

Биометрические персональные данные

сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

Общедоступные персональные данные

персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»;

Иные категории персональных данных

персональные данные, не отнесенные в вышеперечисленным типам.

Виды информационных систем персональных данных в зависимости от категории обрабатываемых в них ПДн



Актуальные угрозы безопасности ПДн

Под **актуальными угрозами** безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать:

уничтожение,
изменение,
блокирование,
копирование,
предоставление,
распространение персональных
данных, а также иные
неправомерные действия.



Типы актуальных угроз

➤ **Угрозы 1-го типа** актуальны для ИС, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в СПО (системном программном обеспечении), используемом в ИС;

➤ **Угрозы 2-го типа** актуальны для ИС, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в ППО (прикладном программном обеспечении), используемом в ИС;

➤ **Угрозы 3-го типа** актуальны для ИС, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

Недекларированные возможности

функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3713

Выдан 22 марта 2017 г.
Действителен до 22 марта 2020 г.

Настоящий сертификат удостоверяет, что операционная система «Альт Линукс СПТ 7.0», разработанная ООО «Базальт-СПО» и производимая ОАО «АВСиЭл-КПО ВС» в соответствии с техническими условиями КИДДС.10514-01ТУ, функционирующая на аппаратных платформах i586 и x86_64, является операционной системой со встроенными средствами защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 4 классу защищенности, «защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 3 уровню контроля и технических условий при выполнении указанных требований, приведенных в формуляре КИДДС.10514-01.30.01.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Научно-производственное объединение вычислительных систем» (аттестат аккредитации от 21.06.2016 № СЗИ RU.0001.01БИ00.Б009) - техническое заключение от 29.12.2016, и экспертного заключения от 03.02.2017 органа по сертификации ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «АВСиЭл-КПО ВС» (ИНН 1660014361)
Адрес: 420029, Республика Татарстан, г. Казань, Сибирский тракт, д. 34
Телефон: (843) 279-5823

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ООО «Научно-производственное объединение вычислительных систем».

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
22 марта 2017 г.

Определение актуальных угроз

Определение типа угроз безопасности персональных данных, **актуальных для информационной системы, производится оператором с учетом оценки возможного вреда,** проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных»

Ст. 18.1. Меры, принимаемые оператором:

5) оценка вреда, который может быть причинен субъектам ПДн в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

Ст. 19. Меры по обеспечению безопасности ПДн.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности ПДн, актуальные при их обработке в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Критерии, применяемые для определения уровня защищенности персональных данных

Тип ИСПДн (Специальные, Биометрические, Общедоступные, Иные ПДн)

Категория субъектов ПДн (Сотрудники оператора, не являющиеся сотрудниками оператора)

Количество субъектов ПДн (более 100 000 или менее 100 000)

Тип актуальных угроз (1 тип, 2 тип, 3 тип)

На практике принято считать:

1. Для любой ИСПДн всегда актуальны только угрозы 3 типа - угрозы, не связанные с наличием недокументированных (недекларированных) возможностей.
2. Категория субъектов ПДн в ИСПДн «Бухгалтерия и кадры» организации чаще всего – не являющиеся сотрудниками оператора, так как в ИСПДн обрабатываются как ПДн сотрудников оператора, так и ПДн иных лиц, не являющихся сотрудниками оператора (уволенные сотрудники, контрагенты и т.д.)

Порядок определения уровня защищенности ПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

Пример:

Определить уровень защищенности ПДн при их обработке в ИСПДн «Бухгалтерия и кадры» бюджетного учреждения Ханты-Мансийского автономного округа – Югры.

Исходные данные:

Обрабатываются ПДн сотрудников, уволенных сотрудников, родственников сотрудников.

Специальные категории ПДн не обрабатываются (сведения о состоянии здоровья, национальность и др.).

Штатная численность организации 120 человек.

Для системы актуальны угрозы 3-го типа.

ИСПДн «Бухгалтерия и кадры»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

Пример:

Определить уровень защищенности ПДн при их обработке в ИСПДн «Медицинская информационная система» окружного уровня.

Исходные данные:

Обрабатываются ПДн пациентов, мед. персонала.

В системе обрабатываются сведения о состоянии здоровья.

В системе обрабатываются данные о пациентах ХМАО (более 100 000 человек)

Для системы актуальны угрозы 3-го типа.

ИСПДн «Медицинская информационная система»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

Перечень требований для обеспечения требуемого уровня защищенности

Требования	Уровни защищенности			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данные	+	+	+	+
Сохранность носителей персональных данных	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	-

Перечень требований для обеспечения требуемого уровня защищенности

Требования	Уровни защищенности			
	1	2	3	4
Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	-	-	-
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	-	-	-

Примеры реализации требований

Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

ПОЛОЖЕНИЕ

об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

Перечень помещений, в которых осуществляется обработка персональных данных

Перечень должностей, доступ которых в Помещения необходим для выполнения ими должностных (трудовых) обязанностей



Примеры реализации требований

Обеспечение сохранности носителей персональных данных



ЖУРНАЛ

учета машинных носителей
персональных данных

Начат _____

Окончен _____

ЖУРНАЛ

учета хранилищ

Начат _____

Окончен _____

Примеры реализации требований

Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Примеры реализации требований

Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз



Примеры реализации требований

Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в ИСПДн

ПРИКАЗ
О назначении ответственного
за обеспечение безопасности
персональных данных в
информационной системе
персональных данных

Примеры реализации требований

Необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей



ID	Время	Пользователь...	Источник	Результат	Неверный пар...
776	02.04.2019 14:23:14	Администратор	Вход в ОС	ОК	
775	02.04.2019 14:22:52	Администратор	Вход в ОС	Указан...	Jy7*WVm0%4
774	02.04.2019 12:05:59	Администратор	Вход в ОС	Доступ...	
773	02.04.2019 12:05:51	Администратор	Вход в ОС	Указан...	Jy7*WVm0%4
772	02.04.2019 12:04:00	Администратор	Вход в ОС	Указан...	121456
771	02.04.2019 12:03:33	Администратор	Вход в ОС	Указан...	
770	02.04.2019 11:58:04	Администратор	Вход в ОС	Указан...	搜索器v300...
769	02.04.2019 11:57:36	Window Ма...	Вход в ОС	ОК	
768	02.04.2019 11:57:36	Font Driver ...	Вход в ОС	ОК	
767	02.04.2019 11:57:24	Font Driver ...	Вход в ОС	ОК	
766	02.04.2019 11:54:37	Неизвестная...	Вход в ОС	Доступ...	
765	02.04.2019 11:54:34	Администратор	Выход из ОС	ОК	
764	02.04.2019 11:47:38	Window Ма...	Выход из ОС	ОК	
763	02.04.2019 11:47:18	Font Driver ...	Выход из ОС	ОК	
762	02.04.2019 11:46:43	Window Ма...	Вход в ОС	ОК	
761	02.04.2019 11:46:42	Font Driver ...	Вход в ОС	ОК	

Примеры реализации требований

Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе



ID	Время	Пользователь	Компьютер	Роль	Оператор	Комментарий	Операция
43	28.02.2019 10:06:18	LOCAL_SVT...		KL.OpenStart	OK		Удалить группу
43	28.02.2019 10:06:18	LOCAL_SVT...		KL.Admins	OK		Удалить группу
41	28.02.2019 10:06:18	LOCAL_SVT...		AMD.FUEL	OK		Удалить группу
40	28.02.2019 10:06:18	LOCAL_SVT...		WinRMUser...	OK		Создать группу
39	28.02.2019 10:06:18	LOCAL_SVT...		SQLServerSQ...	OK		Создать группу
38	28.02.2019 10:06:18	LOCAL_SVT...		SQLServerM...	OK		Создать группу
37	28.02.2019 10:06:18	LOCAL_SVT...		SQLServerM...	OK		Создать группу
36	28.02.2019 10:06:18	LOCAL_SVT...		SQLServerD...	OK		Создать группу
35	28.02.2019 10:06:18	LOCAL_SVT...		Bitnetad	OK	Описание: Нет = Да	Установить параметры пользователя
34	28.02.2019 10:06:18	LOCAL_SVT...		WDAGUtility...	OK	Описание: Нет = Да	Установить параметры пользователя
33	28.02.2019 10:06:18	LOCAL_SVT...		DefaultAcce...	OK	Описание: Нет = Да	Установить параметры пользователя
32	28.02.2019 10:06:18	LOCAL_SVT...		%	OK	Данные: 1, Данные: 1, Пользователь: ...	Создать пользователя
31	28.02.2019 10:06:18	LOCAL_SVT...		anonymous	OK	Описание: Бюджетирование ресурсов	Установить параметры пользователя
30	28.02.2019 10:06:18	LOCAL_SVT...		api.Server	OK	Описание: Бюджетирование ресурсов	Установить параметры пользователя
29	28.02.2019 10:01:40	Администратор		Bitnetad	OK	Данные: Bitnetad, Данные: Пользователь, ...	Создать пользователя
28	28.02.2019 10:01:33	Администратор		WDAGUtility...	OK	Данные: WDAGUtilityAccount, Данные: Поль...	Создать пользователя
27	28.02.2019 10:01:24	Администратор		DefaultAcce...	OK	Данные: DefaultAccount, Данные: Пользов...	Создать пользователя
26	28.02.2019 09:57:44	LOCAL_SVT...			OK		Создать новую сессию-исключения
25	28.02.2019 09:57:44	LOCAL_SVT...			OK		Создать новую сессию-исключения
24	28.02.2019 09:57:44	LOCAL_SVT...			OK		Создать новую сессию-исключения
23	28.02.2019 09:57:44	LOCAL_SVT...			OK		Создать новую сессию-исключения
22	28.02.2019 09:57:44	LOCAL_SVT...			OK		Создать новую сессию-исключения

Примеры реализации требований

Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности

ПРИКАЗ
О создании отдела по защите
информации

ПОЛОЖЕНИЕ Об отделе информационных технологий

Основными задачами отдела являются:

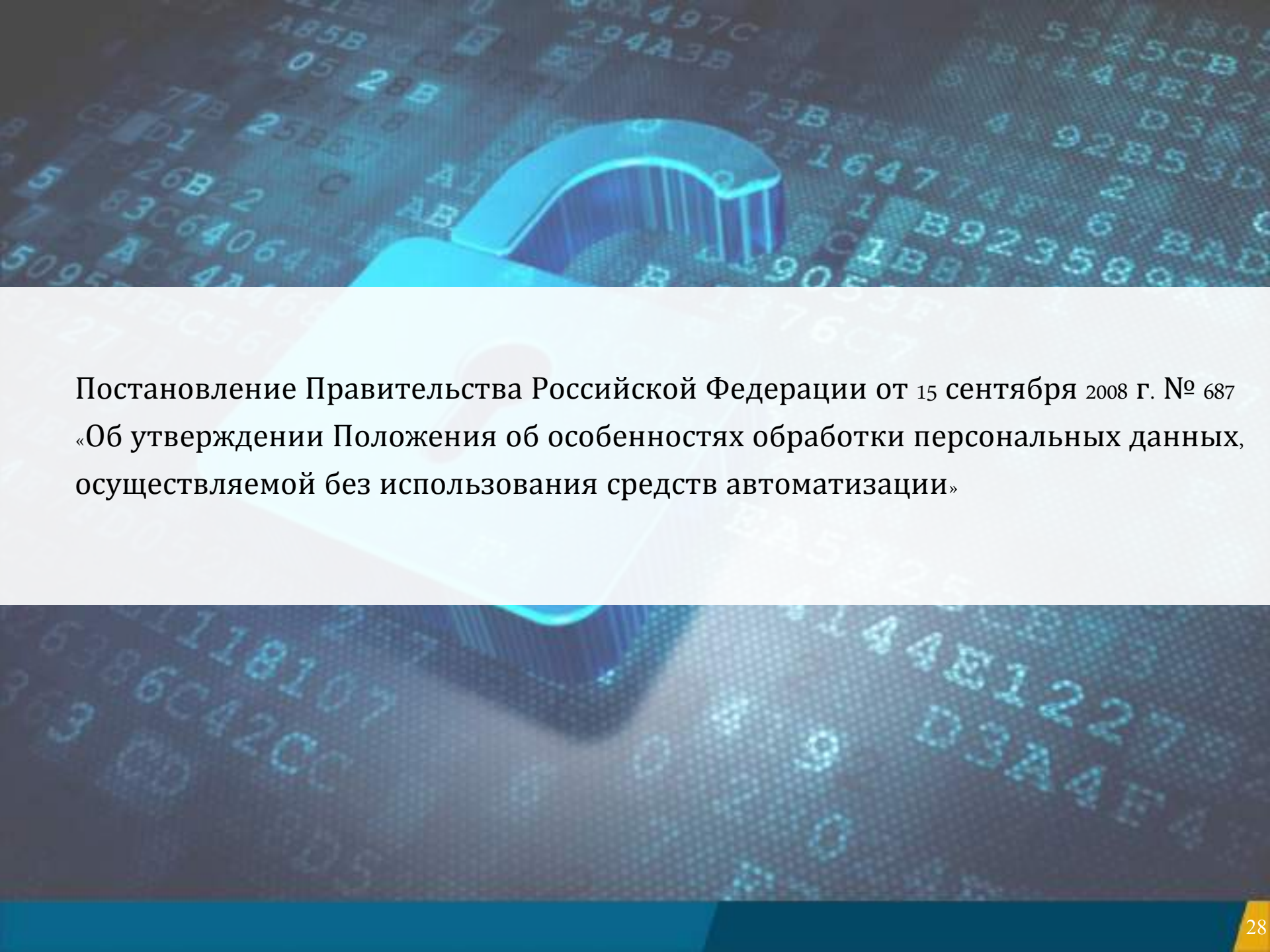
- Обеспечение информационной безопасности информационно-коммуникационной инфраструктуры, информационных систем и ресурсов Учреждения;

- ...

К основным функциям отдела относятся:

- Организация и проведение работ по технической защите информации;

- ...

The background of the slide is a dark blue field filled with glowing, semi-transparent characters from the hexadecimal system (0-9, A-F) and binary code (0-1). These characters are scattered across the entire surface, creating a digital or data-themed aesthetic. In the center of the slide, there is a large, three-dimensional blue padlock. The padlock is oriented horizontally, with its shackle pointing towards the right. It has a metallic texture and is slightly out of focus compared to the text in the foreground. The text is presented in a clean, black, sans-serif font, centered within a white rectangular area that spans the width of the slide.

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687
«Об утверждении Положения об особенностях обработки персональных данных,
осуществляемой без использования средств автоматизации»

Основные положения

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (**неавтоматизированной**), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются **при непосредственном участии человека**.



Основные положения

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.



То есть, если пользователь внес данные в персональный компьютер только для того, чтобы их распечатать, и не сохранял данные на компьютере, то эту обработку можно считать неавтоматизированной. Если пользователь сохранил эти данные в виде файла и хранит их на компьютере, то нужно рассматривать эту обработку ПДн в том числе и как автоматизированную.

Особенности организации обработки ПДн, осуществляемой без использования средств автоматизации

- **Персональные данные** при их обработке, осуществляемой без использования средств автоматизации, **должны обособляться** от иной информации, в частности путем **фиксации** их на **отдельных материальных носителях** ПДн, в специальных разделах или на полях форм (бланков);
- При фиксации ПДн на материальных носителях **не допускается** фиксация на одном материальном носителе персональных данных, **цели обработки** которых **заведомо не совместимы**.

Например,

- хранение в одном месте документов, содержащих ПДн сотрудников и документов, содержащих ПДн граждан, не допускается;
- не допускается хранение в одном месте личных дел сотрудников и уволенных сотрудников;
- личные карточки военнообязанных должны храниться отдельно от личных карточек остальных сотрудников.

Особенности организации обработки ПДн, осуществляемой без использования средств автоматизации

Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), **должны быть проинформированы** о факте обработки ими ПДн, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

ЛИСТ ОЗНАКОМЛЕНИЯ
к Инструкции по обработке
персональных данных без
использования средств
автоматизации

Использование типовых форм документов, содержащих персональные данные

Типовая форма должна содержать:

- сведения о цели обработки ПДн;
- адрес оператора;
- фамилию, имя, отчество и адрес субъекта ПДн;
- источник получения ПДн;
- сроки обработки ПДн;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки персональных данных;
- поле с отметкой о согласии субъекта на обработку ПДн.

Использование типовых форм документов, содержащих персональные данные

- 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Ведение журналов, реестров, книг при организации пропускного режима



Требования к журналам однократного пропуска на объект



Необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена **актом оператора**, содержащим:

- сведения о цели обработки ПДн;
- способы фиксации и состав информации, запрашиваемой у субъектов ПДн;
- перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);
- сроки обработки ПДн,
- порядок пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом персональных данных.



Копирование содержащейся в таких журналах (реестрах, книгах) информации **не допускается**.



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.

Особенности организации обработки ПДн, осуществляемой без использования средств автоматизации

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).



- Каждой категории ПДн должны быть определены места хранения материальных носителей и установлен перечень лиц, осуществляющих обработку либо имеющим к ним доступ.
- Необходимо обеспечить раздельное хранение материальных носителей ПД, обработка которых осуществляется в различных целях.
- При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.



Практические задания

Задание:

Определить уровень защищенности ПДн при их обработке в ИСПДн «Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе - Югре»

Исходные данные:

В системе обрабатываются персональные данные спортсменов, тренеров, организаторов спортивных мероприятий.

В системе обрабатываются помимо иных категорий персональных данных сведения о состоянии здоровья спортсменов.

Объем обрабатываемых персональных данных: менее 100 000 субъектов (спортсмены всех спортивных учреждений округа)

Для системы актуальны угрозы 3-го типа.

ИСПДн «Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе - Югре»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

ИСПДн «Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе - Югре»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	3
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

Задание:

Определить уровень защищенности ПДн при их обработке в ИСПДн «Система контроля и управления доступом»

Исходные данные:

В системе обрабатываются персональные данные сотрудников организации.

В системе обрабатываются ФИО, должность и фотографии сотрудников, которые используются для установления личности сотрудника при проходе на территорию организации.

Штатная численность организации 150 000 человек

Для системы актуальны угрозы 3-го типа.

ИСПДн «Система контроля и управления доступом»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

ИСПДн «Система контроля и управления доступом»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

Задание:

Определить уровень защищенности ПДн при их обработке в ИСПДн «Олимпиадный портал»

Исходные данные:

В системе обрабатываются персональные данные школьников одного муниципального образования (город Ханты-Мансийск).

В системе обрабатываются ФИО, дата рождения, место учебы, информация об участии в олимпиадах и результатах.

Доступ к олимпиадному portalу можно получить только имея учетную запись в системе, открытой части портал не имеет.

Для системы актуальны угрозы 3-го типа.

ИСПДн «Олимпиадный портал»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4

ИСПДн «Олимпиадный портал»

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн «С»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	1	2
		< 100 000	1	2	3
ИСПДн «Б»	Сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	2	3
ИСПДн «И»	Сотрудников	> 100 000	1	3	4
		< 100 000	1	3	4
	Не сотрудников	> 100 000	1	2	3
		< 100 000	1	3	4
ИСПДн «О»	Сотрудников	> 100 000	2	3	4
		< 100 000	2	3	4
	Не сотрудников	> 100 000	2	2	4
		< 100 000	2	3	4