Порядок проведения классификации информационных систем персональных данных

Основные определения

- **Персона́льные да́нные** (или **личные данные**) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

- **Информационная система персональных данных** — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

- **Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Приказ ФСТЭК, ФСБ и Мининформсвязи РФ от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»

Определяет проведение классификации ИСПДн, позволяющих осуществлять обработку персональных данных **с использованием средств автоматизации**

Классификация информационных систем проводится **оператором**

Классификация ИС проводится на этапе их создания или в ходе их эксплуатации с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПД.

Проведение классификации ИС включает в себя следующие этапы:
- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных (Хпд);
- объем обрабатываемых персональных данных (количество субъектов ПД) (Хнпд);
- характеристики безопасности персональных данных обрабатываемых в ИС, заданные оператором;
- структура информационной системы;

- наличие подключений информационной системы к сетям связи общего пользования и (или) сети Интернет;
- режим обработки персональных данных (однопользовательские или многопользовательские системы);
- режим разграничения прав доступа пользователей информационной системы (с разграничением или без разграничения прав доступа);
- местонахождение технических средств информационной системы (в пределах или за пределами РФ).

Категории персональных данных (Хпд)

Категория 4
обезличенные и (или) общедоступные персональные данные.

Категория 3
персональные данные, позволяющие идентифицировать субъекта персональных данных;

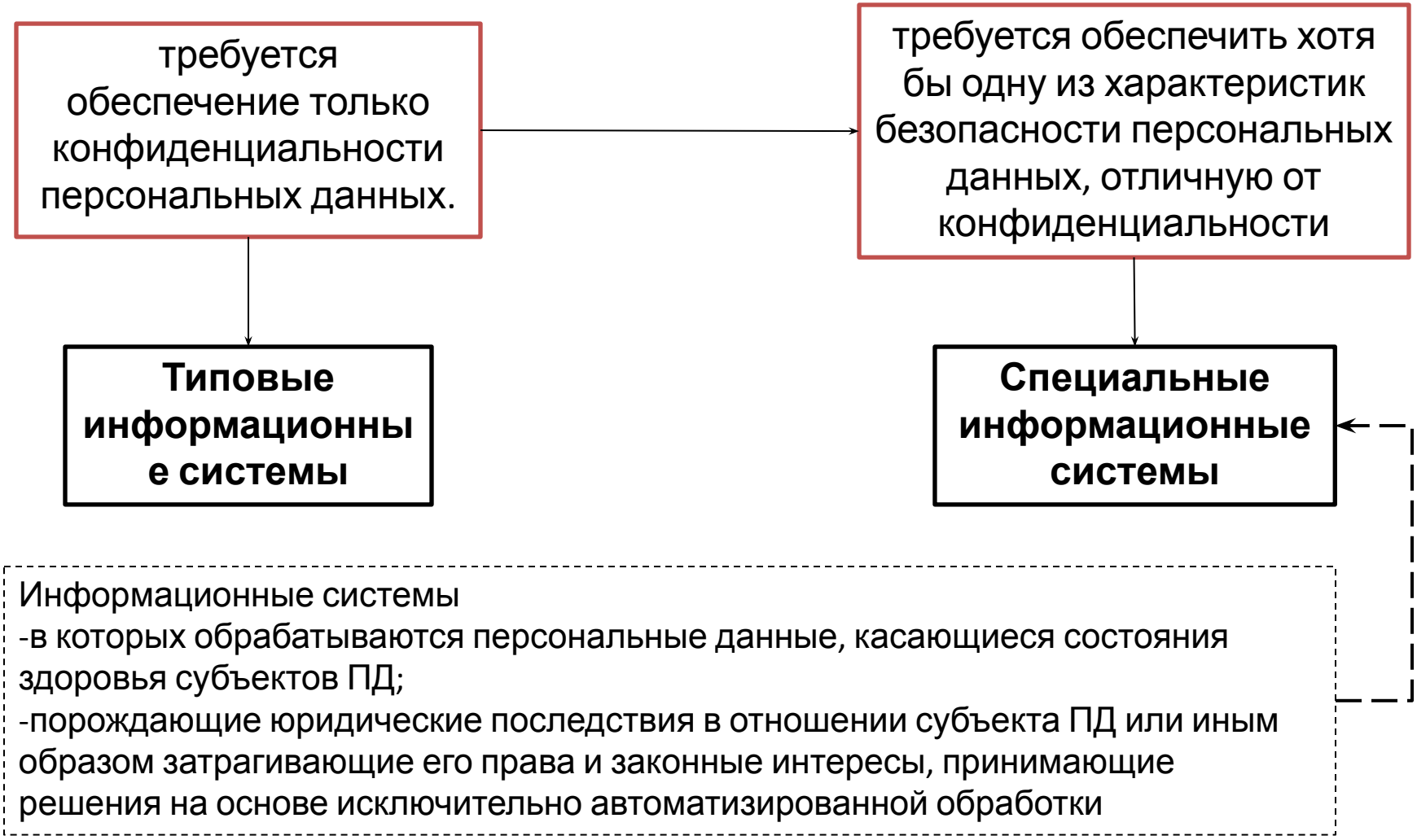
Категория 2
персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

Категория 1
персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Значения объема обрабатываемых персональных данных (Хпдн)

Значение	Примечание
<1 000	Субъектов ПД в пределах конкретной организации;
1 000 – 100 000	Субъектов ПД работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
> 100 000	Субъектов ПД в пределах субъекта Российской Федерации или Российской Федерации в целом.

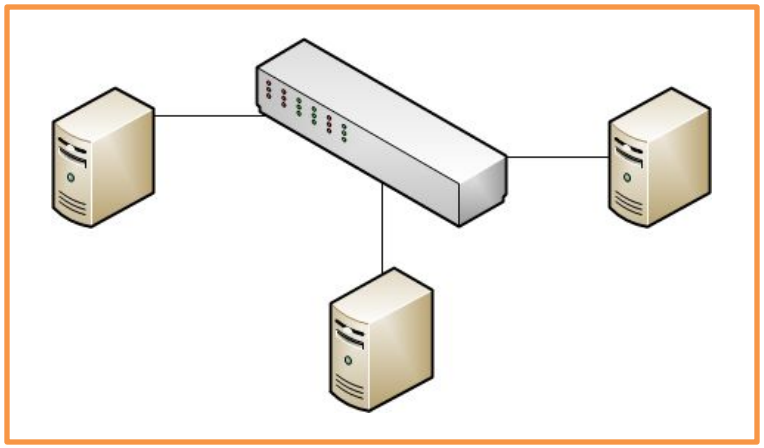
По заданным оператором характеристикам безопасности



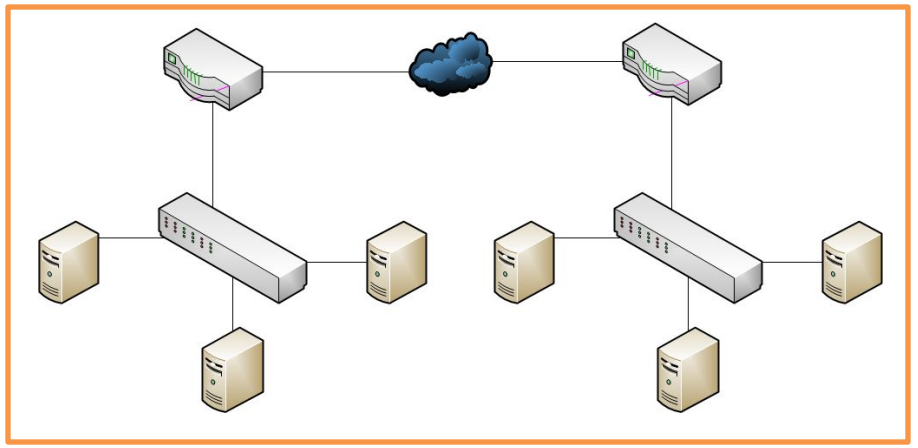
По структуре информационные системы подразделяются:

Автономные
(автоматизированные рабочие места)

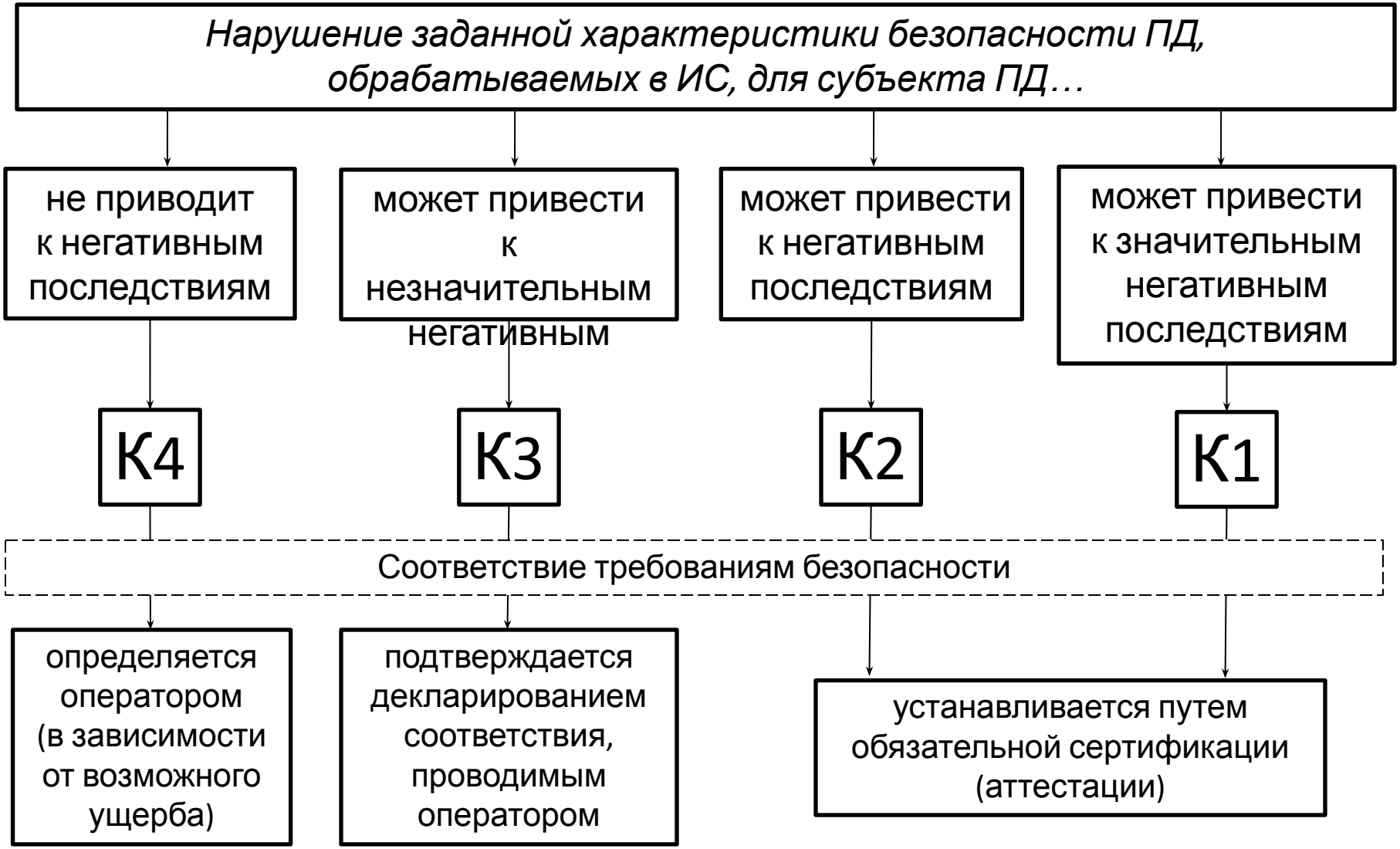
Комплексы автоматизированных рабочих мест
(локальные информационные системы)



Комплексы автоматизированных рабочих мест
(распределенные информационные системы)



По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:



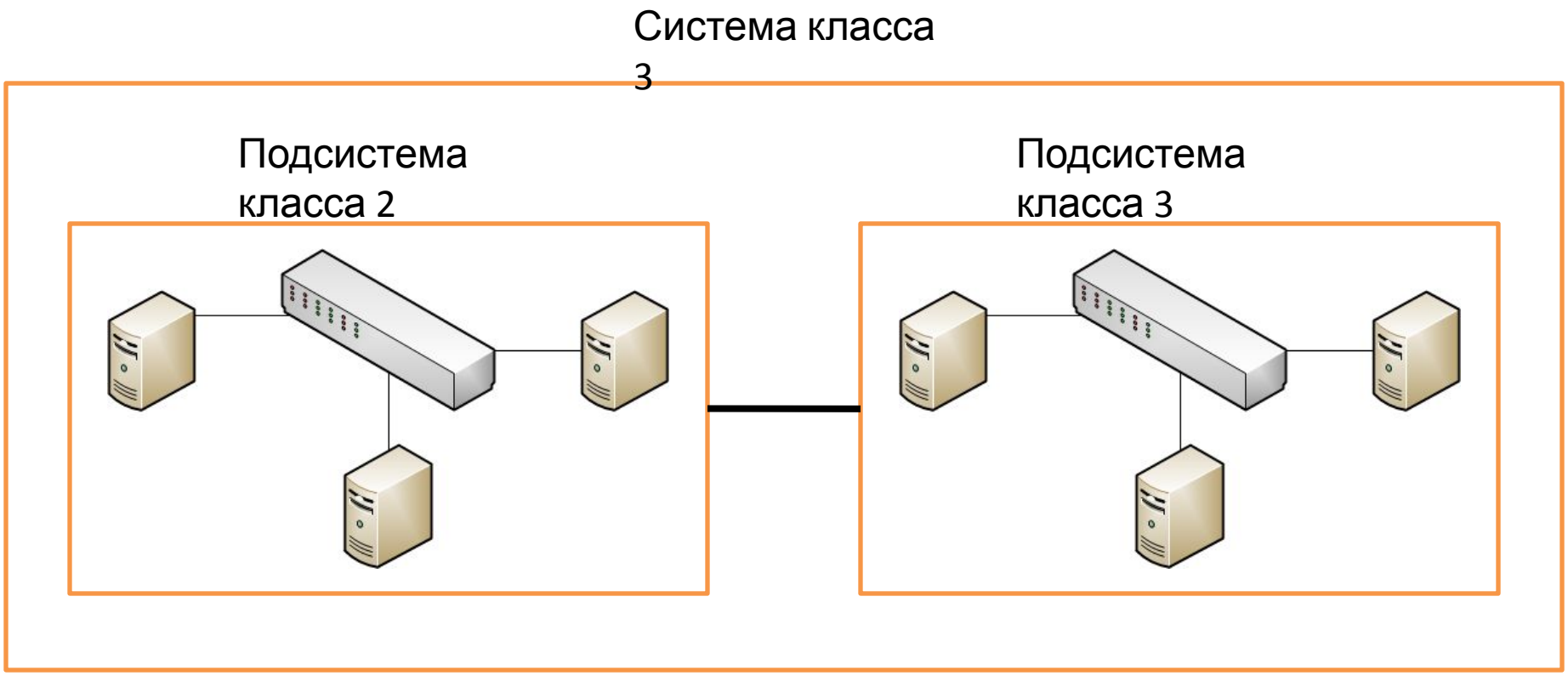
Класс типовой информационной системы определяется в соответствии с таблицей.

	Хпдн		
Хпд	**<1 000**	**1 000 — 100 000**	**> 100 000**
4	К4	К4	К4
3	К3	К3	К2
2	К3	К2	К1
1	К1	К1	К1

**класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».*

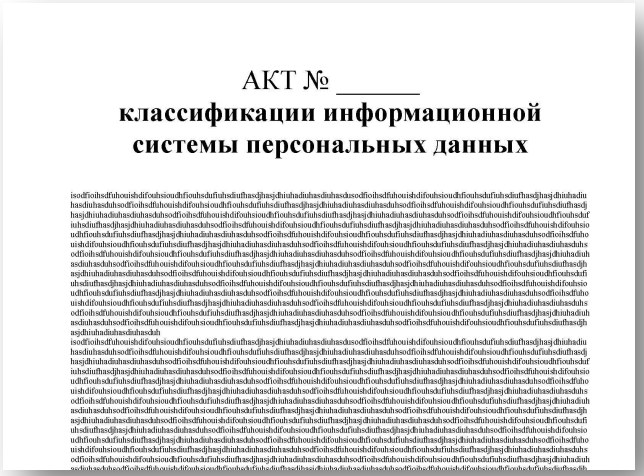
http://lukatsky.blogspot.ru/2012/05/blog-post_21.html

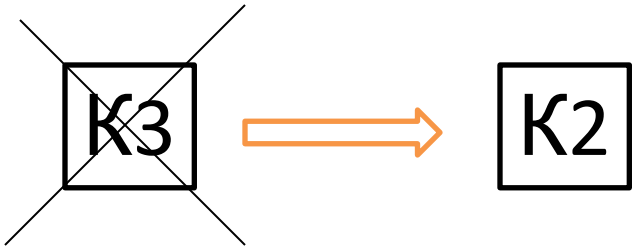
ALSO



$$К_С = MAX(К_{ПС})$$

ALSO


АКТ № _____
классификации информационной
системы персональных данных


К3
К2

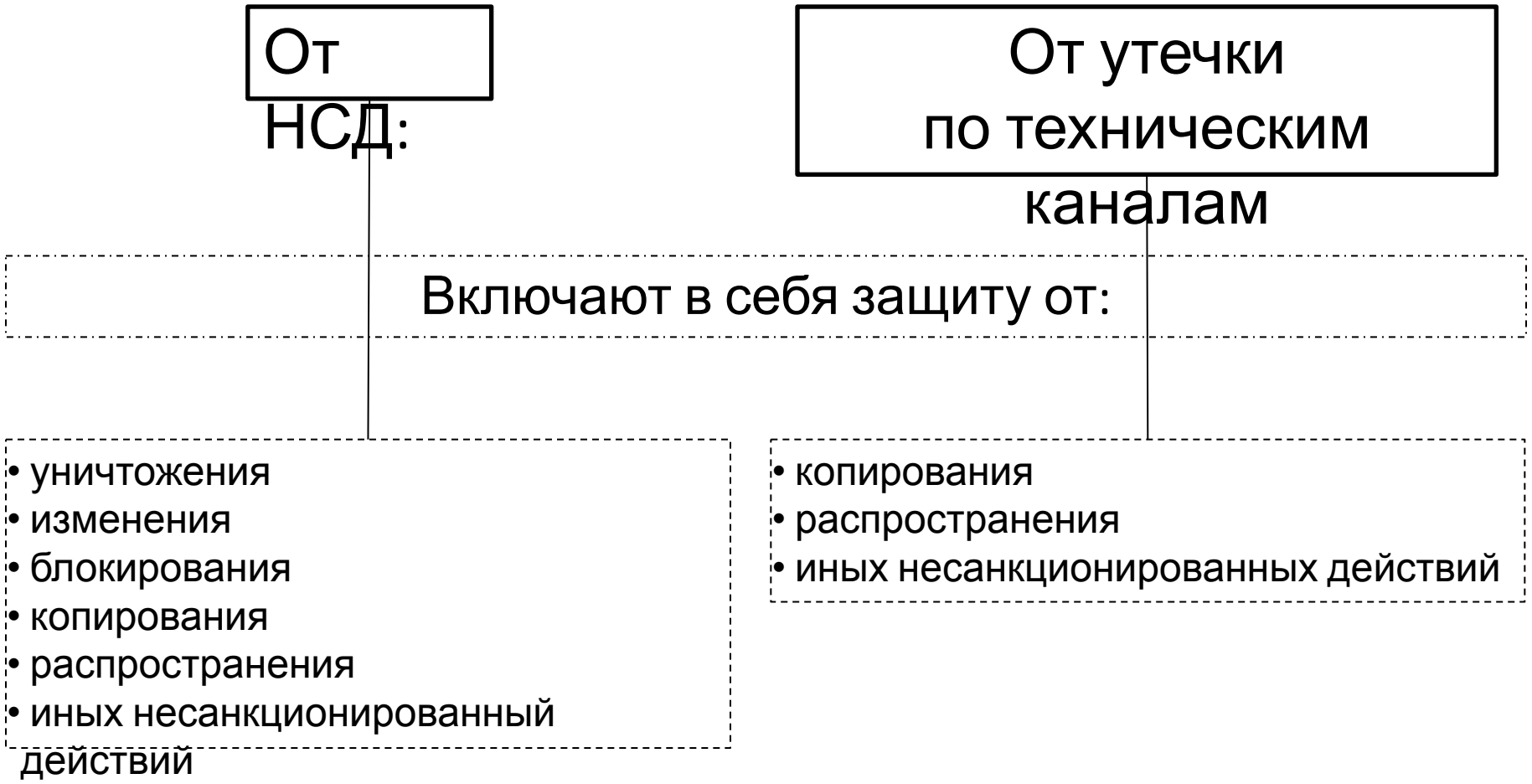
Методы и способы защиты информации в информационных системах персональных данных

Приказ ФСТЭК РФ от 05 февраля 2010 г. №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»

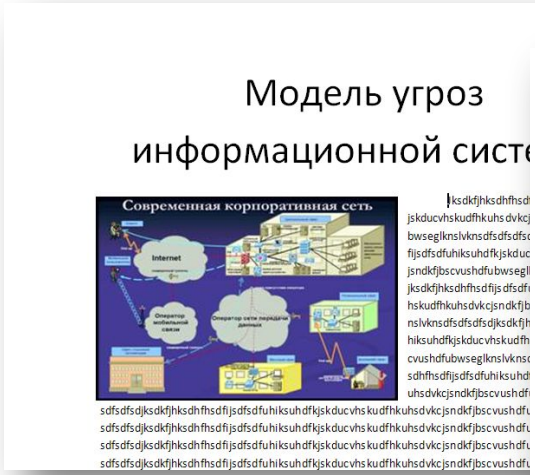
Устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в ИСПДн

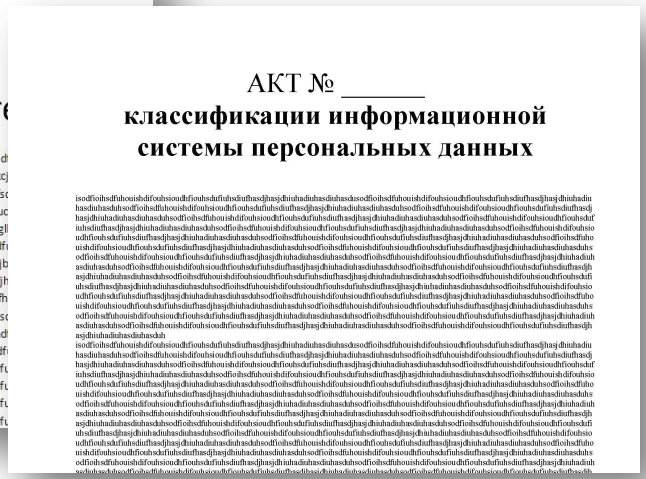
Не рассматривает вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

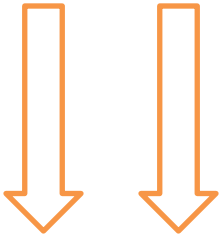
Методы и способы защиты информации:



Выбор и реализация методов и способов защиты информации в ИС:



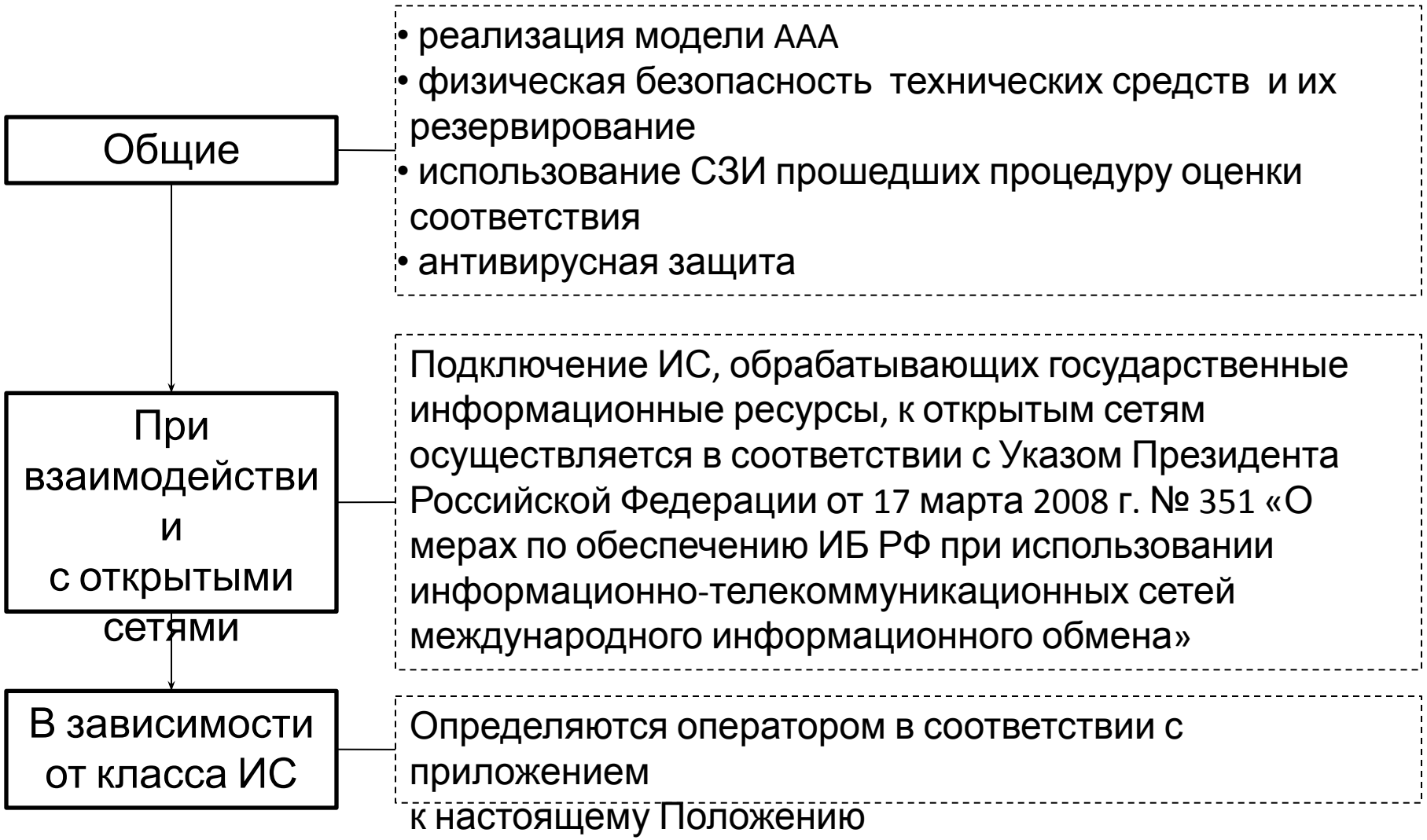




Security Guard

Security Organization

Методы и способы защиты информации от НСД:



Методы и способы защиты информации от НСД:

При взаимодействии с открытыми сетями

Общие

- межсетевое экранирование, фильтрация трафика
- обнаружение вторжений и анализ защищенности ИС , аудит
- использование средств надежной идентификации и аутентификации пользователей
- централизованное управление системой защиты

При наличии удаленного доступа

- проверка подлинности удаленного пользователя и целостности передаваемых данных;
- управление доступом к защищаемым персональным данным информационной сети;
- использование атрибутов безопасности.

При межсетевом взаимодействии и отдельных ИС через открытые сети

- создание канала связи, обеспечивающего защиту передаваемой информации;
- аутентификация взаимодействующих ИС и проверка подлинности пользователей и целостности передаваемых данных;
- обеспечение предотвращения возможности отрицания пользователем факта отправки (получения) ПД другому (от другого) пользователю(я) (для систем разных операторов);

Методы и способы защиты информации от НСД:

К3, К2

	Однопользовательский режим	Многопользовательский режим	
		Равные права	Разные права
управление доступом	- проверка подлинности пользователя при входе в систему по паролю (мин. 6с);	+ идентификатор (код, логин)	==
регистрация и учет	- регистрация входа (выхода) пользователя в систему (из системы), инициализации (останова) ОС и ПО (дата и время); - учет всех защищаемых носителей информации;	+ результат попытки входа (успешная или неуспешная);	+ идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;
обеспечение целостности	- целостность проверяется при загрузке системы по наличию компонентов системы; - физическая охрана информационной системы; - периодическое тестирование функций системы защиты; - наличие средств восстановления системы защиты персональных данных.	==	+ проверка целостности компонентов по контрольным суммам + целостность среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

К1

	Однопользовательский режим	Многопользовательский режим	
		Равные права	Разные права
управление доступом	==	+ идентификация технических средств и каналов связи, внешних устройств по их логическим адресам; + идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;	+ контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
регистрация и учет	+ регистрация выдачи печатных документов на бумажный носитель. (дата и время выдачи, краткое содержание, спецификация устройства выдачи); + дублирующий учет защищаемых носителей информации; + очистка освобождаемых областей оперативной памяти и внешних носителей;	+ идентификатор пользователя, запросившего документ; + регистрация попыток доступа программных средств к защищаемым файлам. + регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа;	==
обеспечение целостности	==	==	==

Безопасное межсетевое взаимодействие с помощью межсетевых экранов

К3	К2	К1
- фильтрация на сетевом уровне для каждого сетевого пакета независимо; - аутентификация администратора межсетевого экрана, учет входа (выхода) его в систему (из системы); - контроль целостности своей программной части; - восстановление свойств межсетевого экрана после сбоев и отказов оборудования; - регламентное тестирование реализации вышеописанных правил.	+ регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации); + регистрация запуска программ и процессов (заданий, задач);	+ фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов; + фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя; + фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя; + фильтрацию с учетом даты и времени; + аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети; + регистрацию и учет запросов на установление виртуальных соединений; + локальную сигнализацию попыток нарушения правил фильтрации; + регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;

Методы и способы защиты информации от утечки по техническим каналам связи:

+

CERTIFICATE

DQS GmbH
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

hereby certifies that the company

custo med GmbH

Leibnizstr. 7
85521 Ottobrunn
Germany

for the scope

design, development, production and service of cardio-pulmonary diagnostic systems such as ECG and blood pressure monitors, stress test systems, spirometers and sleep apnea monitors.

has implemented and maintains a

Quality Management System.

An audit, documented in a report, has verified that this quality management system fulfills the requirements of the following standards:

ISO 13485 : 2003
Quality systems Medical Devices

This certificate is valid until (Expiry date) 2010-12-19

Certificate Registration No. (Unique identification code) 069940 MP23CMDR

Frankfurt am Main (Effective date) 2008-05-13

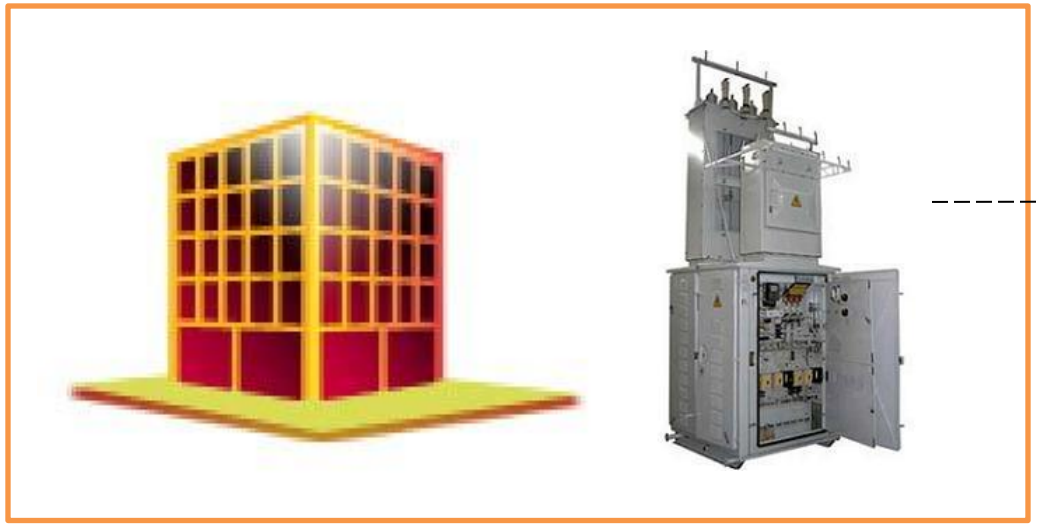
Ass. iur. M. Drechsel
Dipl.-Ing. S. Hemlich
MANAGING DIRECTORS

D-60433 Frankfurt am Main, August-Schanz-Straße 21

DQS is a CMDCAS (Canadian Medical Devices Conformity Assessment System) recognized registrar

+

Методы и способы защиты информации от утечки по техническим каналам связи:



Perimeter