«Бумажная» безопасность

https://yadi.sk/i/_aMwktFyinJXag

Что-то с информацией

- **Приказом утверждаем комиссию по классификации ИС (если нет)**
- **Классифицируем (ИС/ГИС/ИСПДн/КИИ/*)**

Признаки ИС:
информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
(ФЗ 149, статья 2, пункт 3)

Признаки ИСПДН:
информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
(ФЗ 152, статья 3, пункт 10)

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) *(ФЗ 152, статья 3, пункт 1)*

Что-то с информацией

- **Приказом утверждаем комиссию по классификации ИС (если нет)**
- **Классифицируем (ИС/ГИС/ИСПДн/КИИ/*)**

Признаки ГИС:

- должны быть признаки ИС
- **государственные информационные системы** - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании **правовых актов государственных органов** *(ФЗ 149, статья 13, часть 1, пункт 1)*
- **государственные информационные системы** создаются в **целях реализации полномочий государственных органов** и обеспечения обмена информацией между этими органами, а также в иных

Что-то с информацией

- **Приказом утверждаем комиссию по классификации ИС (если нет)**
- **Классифицируем (ИС/ГИС/ИСПДн/КИИ/*)**

Что такое база данных?

- **база данных** (database): Совокупность взаимосвязанных данных, организованных в соответствии со **схемой базы данных** таким образом, чтобы с ними мог работать пользователь *(ГОСТ 34.321-96 п. 2.1)*
- **схема базы данных** (database schema): Формальное описание данных в соответствии с конкретной **схемой данных** *(ГОСТ 34.321-96 п. 2.53)*
- **схема данных** (data schema): Логическое представление организации данных *(ГОСТ 34.321-96 п. 2.54)*

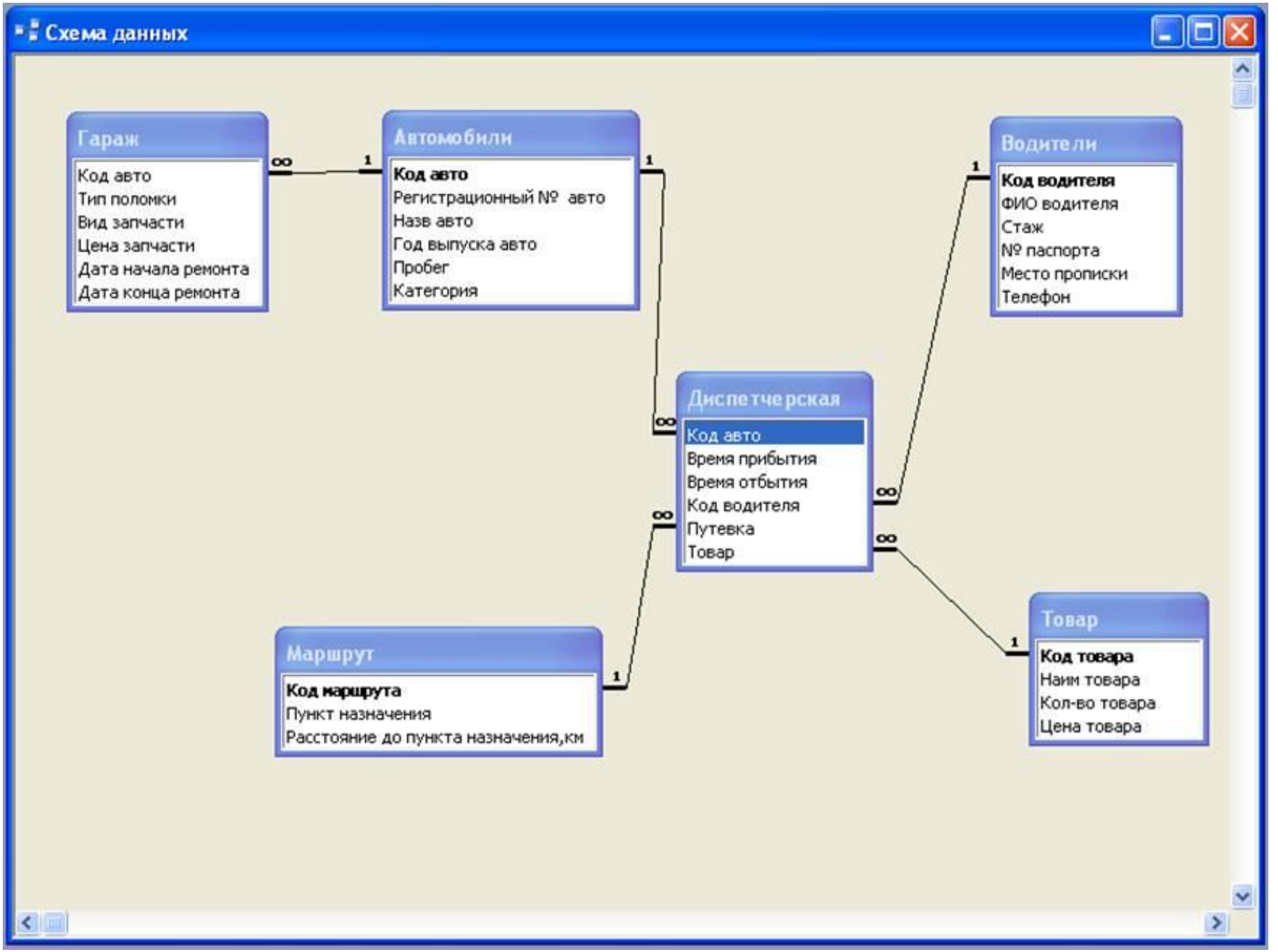
Схема данных
Гараж
Код авто
Тип поломки
Вид запчасти
Цена запчасти
Дата начала ремонта
Дата конца ремонта
Автомобили
Код авто
Регистрационный № авто
Назв авто
Год выпуска авто
Пробег
Категория
Водители
Код водителя
ФИО водителя
Стаж
№ паспорта
Место прописки
Телефон
Диспетчерская
Код авто
Время прибытия
Время отбытия
Код водителя
Путевка
Товар
Маршрут
Код маршрута
Пункт назначения
Расстояние до пункта назначения,км
Товар
Код товара
Наим товара
Кол-во товара
Цена товара
1
∞

Какими документами руководствоваться?

ИСПДН

152 ФЗ

149 ФЗ

Приказ ФСТЭК N 21

ПП N 1119

Приказ ФСБ N 378

ГИС

149 ФЗ

Приказ ФСТЭК N 17

ФСТЭК «Меры защиты информации в государственных информационных системах»

Намеки на документы

2 статьи 19 закона №152-ФЗ «О персональных данных»:

Обеспечение безопасности персональных данных достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных; *(нужна модель угроз)*
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; *(организационные меры по большей части и есть наши документы, плюс здесь отправляют читать дальше подзаконные акты)*

2 статьи 19 закона №152-ФЗ «О персональных данных»:
Обеспечение безопасности персональных данных достигается, в частности:

Намеки на документы

- 5) учетом машинных носителей персональных данных; *(нужен некий журнал учета и правила учета машинных носителей)*
- 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер; *(необходимо разработать правила обнаружения инцидентов и устранения их последствий, возможно, необходимо назначить группу реагирования на инциденты)*
- 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; *(нужны правила резервирования и восстановления)*

2 статьи 19 закона №152-ФЗ «О персональных данных»:
Обеспечение безопасности персональных данных достигается, в частности:

Намеки на документы

- 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; *(разработка системы допуска к данным, можно сделать на основе ролей в системе, так же само программное обеспечение должно уметь вести логи кто когда и к каким данным обращался)*
- 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных. *(нужен план периодического контроля, плюс, возможно журнал, в котором будут фиксироваться результаты такого контроля)*

Группы документов

- **Общее** – документы для ИСПДн, ГИС, КИИ
- **Только ГИС** – документы для ГИС или муниципальных
- **ПДн** – документы по защите ПД и во исполнение законодательства по защите ПД.
- **СКЗИ** – документы для исполнения нормативных документов ФСБ, разрабатываются для всех систем, в которых применяются сертифицированные СКЗИ

1. Приказ о назначении ответственных лиц и инструкции этим лицам

(ФЗ 152, пункт 18.1)

1. Оператор обязан принимать меры… К таким мерам могут, в частности, относиться:
1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

(приказ ФСТЭК N17, пункт 9)

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.
Администратор безопасности.

Общие

2. Приказ о назначении группы реагирования на инциденты информационной безопасности (ГРИИБ) и инструкция по реагированию (РСБ.1, РСБ.2)

(ГОСТ Р ИСО/МЭК ТО 18044-2007 п. 3.4)
группа реагирования на инциденты информационной безопасности (ГРИИБ) (Information Security Incident Response Team (ISIRT)): Группа обученных и доверенных членов организации.

(ФЗ 152, статья 19)
Меры по обеспечению безопасности персональных данных при их обработке

(Приказ ФСТЭК N17, статься 18.2)
В ходе выявления инцидентов и реагирования на них осуществляются: …

Общие

3. Инструкция пользователя

(ФЗ 152, статья 18.1)

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, **и (или) обучение указанных работников.**

Общие

4. Политика информационной безопасности (РСБ.1, РСБ.2)

(ФЗ 152, статья 18.1)

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, **и (или) обучение указанных работников.**

4. Политика информационной безопасности
(УПД.2, УПД.3 , УПД.4, ОПС.3, ОДТ.3, ОДТ.4)

Порядок резервирования
(ФЗ 152, статья 19, часть 2)
Обеспечение безопасности персональных данных достигается, в частности:
7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

(Приказ ФСТЭК N21)
ОДТ.4 Периодическое резервное копирование информации на резервные машинные носители

Общие

5. Приказ о контролируемой зоне и положение о контролируемой зоне (ЗТС.2)

(Приказ ФСТЭК 17/21 ЗТС.2)

«Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования».

МЧС РОССИИ

53 ПСЧ
ФЕДЕРАЛЬНОЕ КАЗЕННОЕ
УЧРЕЖДЕНИЕ
«8 ОТРЯД ФЕДЕРАЛЬНОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ ПО ЯМАЛО-НЕНЕЦКОМУ АВТОНОМНОМУ ОКРУГУ (ДОГОВОРНОЙ)»

Журнал учета журналов лежащих в куче других журналов

Общие

Журналы

- Журнал учета стационарных машинных носителей
- Журнал учета портативных устройств
- Журнал учета съемных МНИ
- Журнал учета СрЗИ
- Журнал периодического тестирования СрЗИ
- Журнал инструктажей по ИБ
- Журнал учета мероприятий по ИБ

Только ГИС

1. Приказ необходимости защиты информации

(Приказ ФСТЭК 17, пункт 14)

принятие решения о необходимости защиты информации, содержащейся в информационной системе

2. Приказ о классификации и акт классификации

(Приказ ФСТЭК 17, пункт 14)

классификацию информационной системы по требованиям защиты информации

Только ГИС

3. Приказ о вводе в действие

(Приказ ФСТЭК 17, пункт 17.5)

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

ПДн

1. Положение о защите и обработке ПДн

(ФЗ 152, ПП 1119)

Ключевые разделы положения:

- определение перечня обрабатываемых персональных данных
- общие принципы обработки
- порядок сбора и хранения персональных данных
- процедура получения персональных данных работников
- передача персональных данных третьим лицам
- трансграничная передача персональных данных
- порядок уничтожения и блокирования персональных данных
- защита персональных данных
- согласие на обработку персональных данных
- права и обязанности организации и работников

ПДн

2. Приказ об утверждении перечня лиц, допущенных к обработке ПДн

(ФЗ 152)

3. Политика в отношении обработки персональных данных

(ФЗ 152, статьи 18.1, часть 2)

Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. …

4. Приказ об определении уровня защищенности и акт

(ПП 1119, ФЗ 152, статьи 19, часть 3)

требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

ПДн

4. Форма согласия субъекта на обработку его ПДн

(ФЗ 152, статья 9, часть 4)

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. …

ПД
н

5. Форма соглашения о неразглашении персональных данных

(ФЗ 152, статья 19, часть 1)

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

СКЗИ

Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации,…»

Приказ ФСБ РФ от 9 февраля 2005 г. N 66
«Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Приказ ФАПСИ от 13 июня 2001 г. N 152
«Об утверждении 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»

СКЗИ

Приказ о порядке хранения и эксплуатации средств криптографической защиты информации (СКЗИ)
(ФАПСИ 152)

Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов
(ФАПСИ 152)