Сессия 2. «Стратегические сценарии научно-методического сопровождения проектов формирования единой цифровой образовательной среды»

Тема: Информационная безопасность в условиях цифровой трансформации образования

Гнедков Андрей Владимирович,
Начальник отдела
обеспечения информационной безопасности
ГБУ ДПО «ЧИРО»

Челябинск
30 ноября - 1 декабря 2023 года

Информация

Информация - сведения (сообщения, данные) независимо от формы их представления. [1]

Кто владеет информацией, тот владеет целым миром. [2]

1. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
2. Натан Майер Ротшильд.

Информационная безопасность

Система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере представлена в Доктрине информационной безопасности Российской Федерации. [3]

Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. [4]

Информационная безопасность организации - состояние защищенности (обеспечение конфиденциальности, целостности и доступности информации) интересов организации в условиях угроз в информационной сфере. [5]

3,4. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
5. ГОСТ Р 53114-2008. "Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения".

Направления в области информационной безопасности

Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются [6]:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

6. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

Стратегическое направление в области цифровой трансформации образования

Целью стратегического направления в области цифровой трансформации образования является достижение высокой степени "цифровой зрелости" сферы образования на базе единого, качественного, **безопасного образовательного пространства**, построенного с учетом предоставления равного доступа к качественному верифицированному цифровому образовательному контенту и цифровым образовательным сервисам на всей территории Российской Федерации для всех категорий участников образовательных отношений. [7]

7 - Распоряжение Правительства РФ от 18.10.2023 N 2894-р

Основной инструмент реализации мероприятий в области цифровой трансформации

Основным инструментом реализации мероприятий в области цифровой трансформации общего и среднего профессионального образования является федеральный проект "Цифровая образовательная среда" национального проекта "Образование", в рамках которого **обеспечивается формирование инфраструктуры и материально-технической базы** образовательных организаций для создания условий, которым должна соответствовать современная образовательная организация, в том числе в целях формирования качественно нового уровня процесса получения знаний. [8]

8 - Распоряжение Правительства РФ от 18.10.2023 N 2894-р

Информационные системы

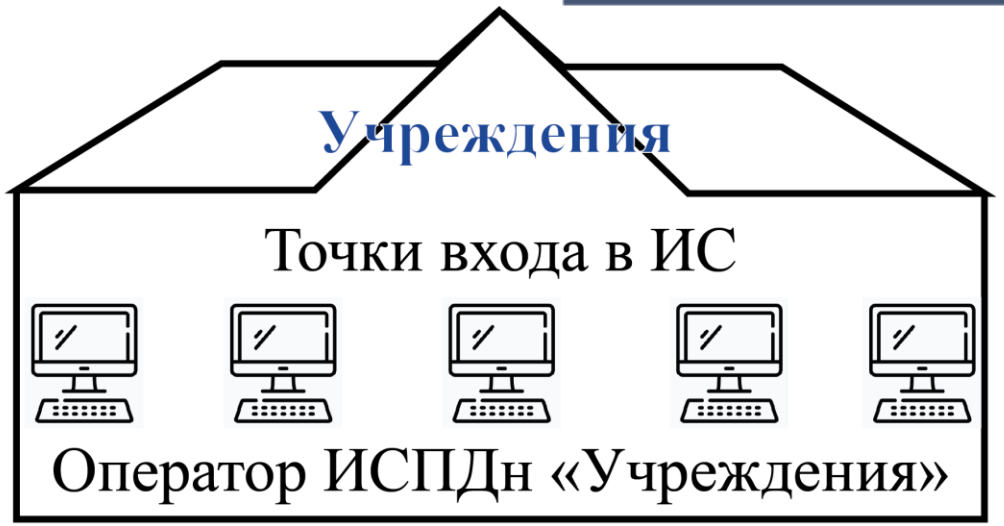
Ключевой системой стала федеральная государственная информационная система "Моя школа".

Также в рамках реализации федерального проекта "Цифровая образовательная среда" разработана и развивается информационно-коммуникационная образовательная платформа "Сферум".

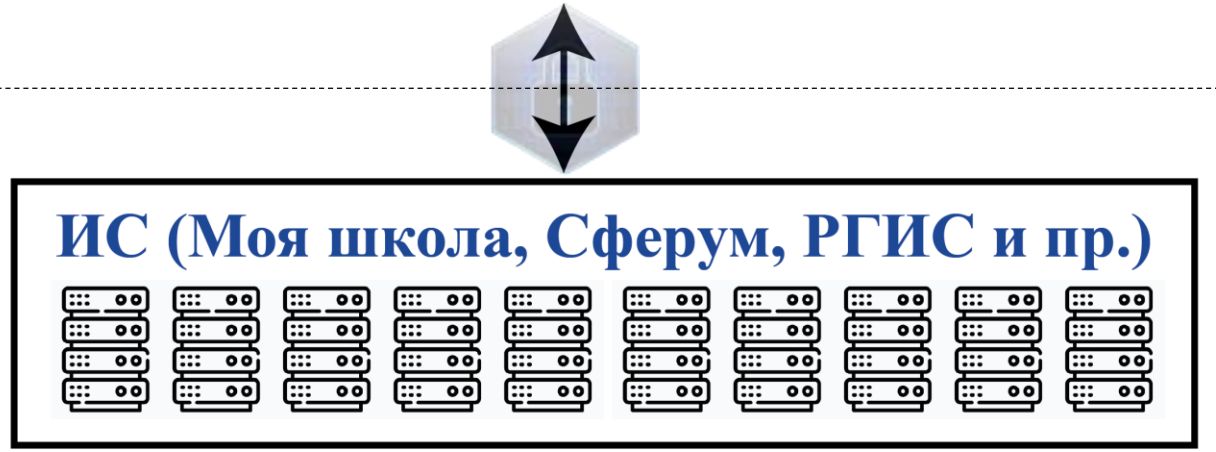
В целях предоставления государственных и (или) муниципальных услуг учреждения используют региональные государственные информационные системы.

Работа с информационными системами

Информационная безопасность (ИБ) со стороны учреждения



ИБ со стороны операторов ИС



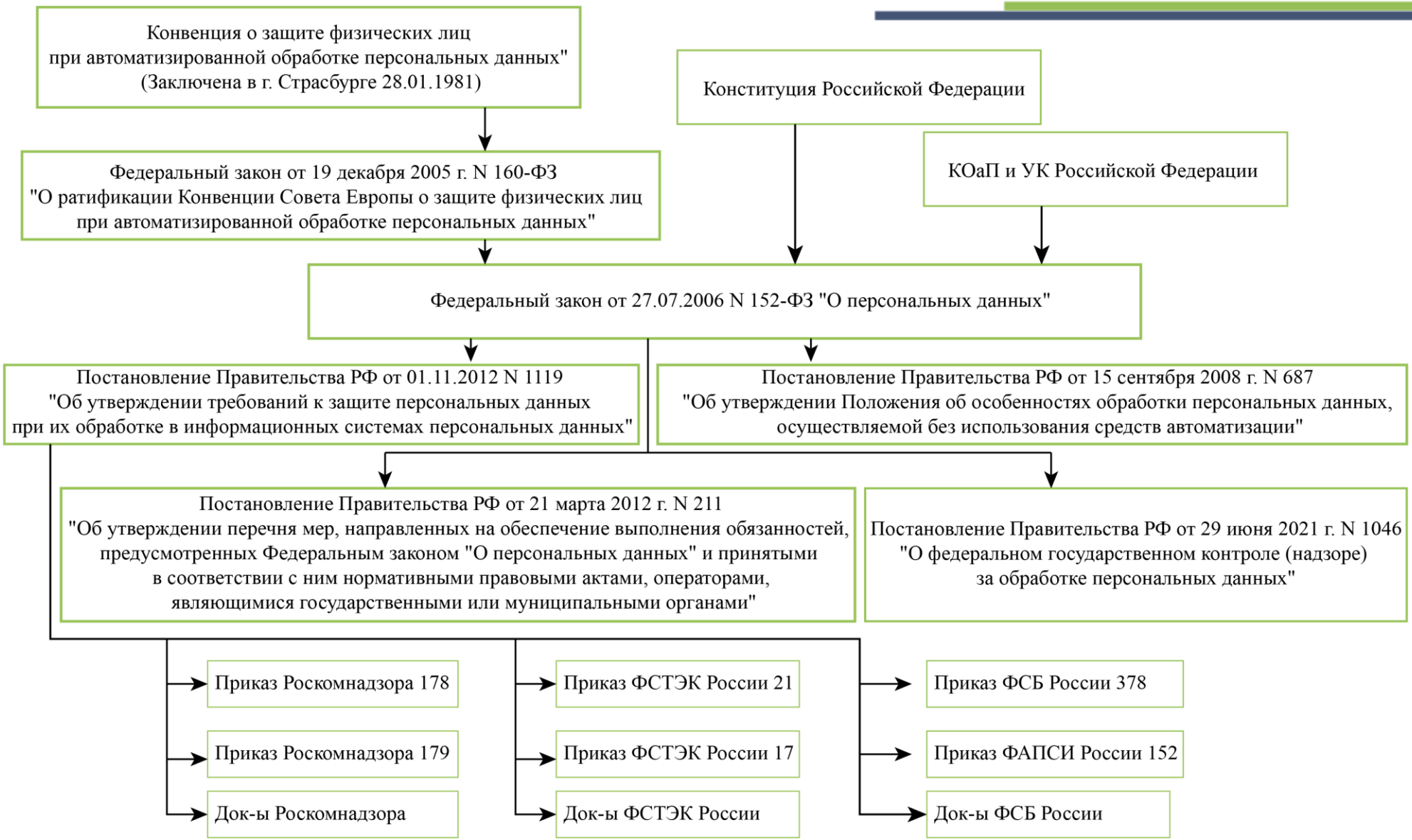
ИБ со стороны пользователей ИС

Педагогические работники, дети и их законные представиетли

Информационная безопасность со стороны учреждений и операторов ИС

Со стороны **учреждений** и **операторов ИС** информационная безопасность достигается применением правовых, организационных и технических мер защиты информации в соответствии с нормативными правовыми актами Российской Федерации.

Визуализация системы НПА в области персональных данных



Обязанности операторов

Федеральный закон от 27.07.2006 №152 «О персональных данных»

Глава 4

Обязанности оператора

Пункт 4 часть 2 статья 19

Обеспечение безопасности ПДн достигается **оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.**

Пункт 2 часть 2 статья 19

Обеспечение безопасности ПДн достигается 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.

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Пункт 17 Требований..

Контроль за выполнением требований организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по ТЗКИ. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Пункт 6 Состава и содержания..

Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по ТЗКИ. Указанная оценка проводится не реже одного раза в 3 года.

Информационная безопасность со стороны пользователей ИС

Со стороны **пользователей ИС** информационная безопасность достигается за счёт культуры личной информационной безопасности граждан (кибергигиена).

Правила кибергигиены

1. Не писать пароли на стикерах и не сохранять в файлах на компьютере, не произносить их вслух при вводе. Если коллега по работе или посетитель запомнит пароль со стикера, отвечать за их действия придется его владельцу.

2. Не «запоминать» пароли в браузерах и не использовать одинаковые пароли для разных систем. Да, это удобно, но небезопасно: злоумышленники специально создают вирусы и программы для взлома такого ПО, чтобы похищать пароли и использовать в своих целях.

3. Использовать надежные пароли. Пароли вида «123456» подберёт даже школьник. Если будете использоваться надежный пароль (цифры, заглавные и строчные буквы, специальные символы, длина не менее 8 символов) то вероятность подбора такого пароля будет низкая.

4. Не передавать свои учётные данные (логин/пароль) третьим лицам. За все действия таких лиц, ответственность будет нести их владелец.

5. Скачивать приложения только из доверенных источников: с официального сайта производителя или из официальных магазинов приложений.

6. Использовать антивирусное ПО для защиты информации, особенно при работе в сети «Интернет», а также прочие средства защиты информации.

Итог

Цифровизация системы образования несёт в себе дополнительные риски, связанные с обеспечением конфиденциальности, целостности и доступности обрабатываемой информации.

Информационная безопасность в условиях цифровой трансформации образования является её неотъемлемой частью и обеспечивается принятием правовых, организационных и технических мер со стороны учреждений и операторов ИС, а также соблюдением элементарных правил при работе с такими ИС со стороны её пользователей.

Сессия 2. «Стратегические сценарии научно-методического сопровождения проектов формирования единой цифровой образовательной среды»

Тема: Информационная безопасность в условиях цифровой трансформации образования

Гнедков Андрей Владимирович,
Начальник отдела
обеспечения информационной безопасности
ГБУ ДПО «ЧИРО»

Челябинск
30 ноября - 1 декабря 2023 года