

Медиагигиена и работа с информацией в цифровой образовательной среде

ФГАНУ «ФИЦТО»

Содержание вебинара



Цель - информирование педагогических работников и технических специалистов образовательных организаций об обеспечении информационной безопасности личности в цифровой образовательной среде.



- ❖ Гигиенический аспект правил организации и реализации обучения в условиях цифровой образовательной среды, основные организационные требования к электронным образовательным ресурсам.
- ❖ Социально-правовой аспект обеспечения защиты личных данных детей в цифровой образовательной среде.
- ❖ Информационная безопасность, контролируемая пользователем.
- ❖ Информационная безопасность в рамках ФГИС “Моя школа”.

Информационная безопасность личности в цифровой образовательной среде



Гигиенический аспект правил организации и реализации обучения в целях обеспечения безопасного информационного взаимодействия в цифровой образовательной среде

- гигиенические аспекты, правила организации и реализации обучения в условиях информационной образовательной среды,
- основные организационные требования к электронным образовательным ресурсам.

Цифровая образовательная среда
совокупность научно-методических и организационно-технологических условий, обеспечивающих информационное взаимодействие между субъектами образовательного процесса и интерактивным информационным ресурсом, на основе реализации возможностей информационных и коммуникационных технологий (как аналоговой, так и цифровой формы реализации)

Социально-правовой аспект обеспечения защиты личных данных детей

- основные угрозы информационной безопасности для детей,
- обеспечение защиты личных данных детей,
- основные НПА, обеспечивающие информационную безопасность личности.

Информационная безопасность, контролируемая пользователем

Информационная безопасность в рамках ФГИС "Моя школа"



**Социально-
правовой
аспект обеспечения
защиты личных
данных детей**



Боков Денис Юрьевич,
кандидат философских наук,
советник ФГАНУ «Федеральный
институт цифровой трансформации
в сфере образования»



Персональные данные

любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

*Статья 3 Федерального закона
от 27.07.2006 № 152-ФЗ «О персональных
данных»*

Личные данные

любая обрабатываемая лицом в электронном виде информация, неправомерной доступ к которой может повлечь негативные последствия, при этом которая явным образом может не относиться к персональным данным

Основные нормативные правовые акты в сфере информационной безопасности детей



Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203

Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400

Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Пример личных данных в сфере информационной безопасности детей



- Пространственная локализация
- Идентификационные (учетные) данные
- Хроника личных событий
- Интеллектуальные и психологические особенности (умения, навыки, личностные черты)
- Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам)
- Материально-экономическое положение (достаток в семье)
- Образ жизни и поведенческие установки (мировоззрение, социальные привычки и действия)

Основные объекты, используемые для реализации неправомерного доступа в сфере информационной безопасности детей



- Облачные сервисы хранения информации
- Личные мобильные устройства
- Устройства, которые временно использовались для входа на сервисы и ресурсы в сети «Интернет»
- Персональные компьютеры

Виды угроз информационной безопасности детей



- Угрозы вреда детям от информации, причиняющей вред их здоровью и развитию
- Угрозы, связанные с мошенническими действиями или вредоносным программным обеспечением, распространяемым через сеть «Интернет»
- Угрозы неправомерного доступа к персональным и личным данным детей:
 - размещенных детьми и их родителями на ресурсах и сервисах в сети «Интернет»
 - обрабатываемых государственными организациями
 - хранимых на мобильных устройствах и персональных компьютерах

Рекомендации для детей по установлению пароля



- Пароль должен быть сложным. Сложный пароль состоит из минимум восьми символов, включая большие и маленькие буквы, цифры и специальные символы. Пример такого пароля: «oPQ0nz\$Hx4%!»
- Не составляйте пароль из личных данных и очевидных слов, фраз или наборов символов
- Для каждого сайта необходимо создавать отдельный пароль.
Использовать один и тот же пароль для нескольких сайтов небезопасно
- Для того, чтобы не забыть большое количество сложных паролей:
 - ✓ возьмите за основу стихотворение или фразу, запишите строчными и прописными латинскими буквами
 - ✓ возьмите легко запоминающееся выражение. Используйте первую букву каждого слова из выражения, примените прописные буквы и дополните цифрами (можно использовать телефонный код или почтовый индекс, записанный в обратном порядке)
- Для того, чтобы запомнить, какой пароль для какого сайта вы создали, – добавьте в пароль адрес страницы, для которой он вам нужен, например, первую и третью буквы названия страницы и вторую букву после точки (MS - myschool)



Информационная безопасность в рамках ФГИС “Моя школа”



Маслобойников Юрий,
начальник отдела эксплуатации
компонентов ФГАНУ «ФИЦТО»

Основные понятия



**Федеральная государственная информационная система «Моя школа»
(ФГИС «Моя школа»)
Подсистема информационной безопасности (ПИБ)**

первый класс защищённости (К1)

третий уровень защищённости обрабатываемых персональных данных (УЗ-3)

НПА:

- Федеральный закон от 27.07.2006 № 152-ФЗ "О 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"
- Приказ ФСТЭК РФ 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"
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
- Федеральный закон от 06.07.2015 № 676 "О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации"
- Приказ ФСТЭК РФ от 11.02.2013 № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Цели ПИБ:

- нейтрализация всех актуальных угроз безопасности информации;
- выполнение требований нормативно-правовых актов Российской Федерации, руководящих и методических документов ФСТЭК и ФСБ России

Задачи ПИБ:

- исключение неправомерного доступа к информации (обеспечение конфиденциальности)
- исключения неправомерного уничтожения или модифицирования информации (обеспечения целостности)
- исключения неправомерного блокирования информации (обеспечение доступности)

Взаимодействие с ЕСИА и ГИС РУО



Пользователи



Авторизация пользователей
в ЛК ФГИС "Моя школа" через ЕСИА
(Портал госуслуг)



Получение согласия на передачу
данных из Платформы согласия
ЕСИА



Автоматизированный запрос в ГИС
РУО сведений по данным из ЕСИА



Возврат из дневника в ЛК Моя школа:
оценки, Д/З, расписание.
Отображение ФИО пользователя из
ЕСИА



Запрос в региональный дневник
по ID ЕСИА

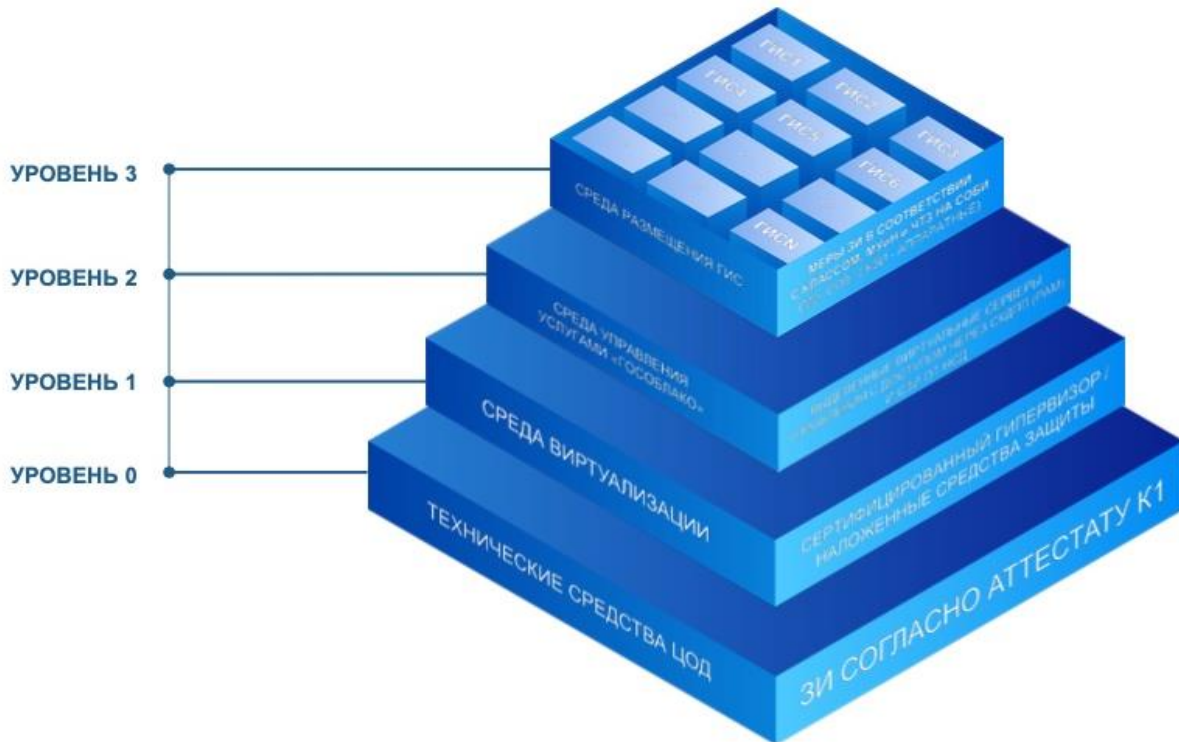


Возврат из ГИС РУО во ФГИС
«Моя школа»: регион, школа,
(название, адрес), класс, роль



Логика обеспечения ИБ на платформе ГЕОП

ТРЕБОВАНИЯ ПРИКАЗА № 17 ФСТЭК РОССИИ



Меры ЗИ, реализуемые на платформе «ГосОблако»:

ИАФ (идентификация и аутентификация субъектов доступа и объектов доступа)

УПД (управление доступом субъектов доступа к объектам доступа)

ОПС (ограничение программной среды)

ЗНИ (защита машинных носителей информации)

РСБ (регистрация событий безопасности)

АВЗ (антивирусная защита)

СОВ (обнаружение вторжений)

АНЗ (контроль (анализ) защищенности информации)

ОЦЛ (обеспечение целостности информационной системы и информации)

ОДТ (обеспечение доступности информации)

ЗСВ (защита среды виртуализации)

ЗТС (защита технических средств)

ЗИС (защита информационной системы, ее средств и систем связи и передачи данных)



Меры применяемые для обеспечения конфиденциальности



Российские ОС

Для функционирования ПО ФГИС используются отечественные операционные системы



Сертифицированные СУБД

Для функционирования ПО ФГИС используются сертифицированные системы управления базами данных



Защита от НСД

Для функционирования ПО ФГИС используются сертифицированные отечественные средства защиты от несанкционированного доступа



Меры применяемые для обеспечения целостности



Организационные

- регламенты проведения обслуживания
- обеспечение контроля за эксплуатацией



Технические

- логирование действий пользователей
- мониторинг событий информационной безопасности
- резервное копирование





Технические меры применяемые для обеспечения доступности



Внедрение ФГИС «МОЯ ШКОЛА»



Постановление Правительства РФ от 13 июля 2022 г.
№ 1241 «О федеральной государственной информационной
системе «Моя школа»»

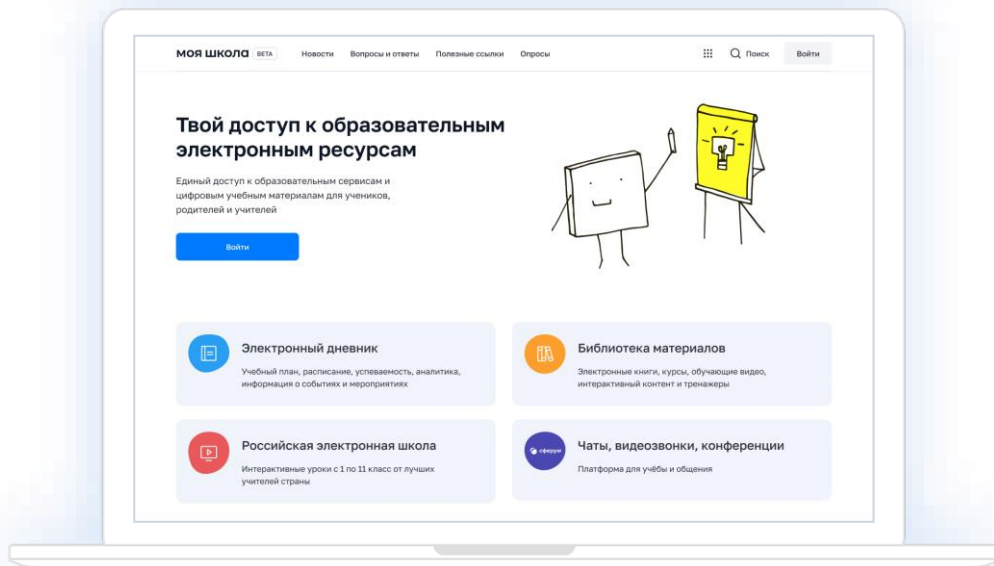
с 1 сентября 2022

заработал единый доступ к образовательным сервисам
и цифровым учебным материалам ФГИС «Моя школа»
для учеников, родителей и учителей.

Аттестат соответствия ФГИС «Моя школа» требованиям по
защите информации от 01.09.2022 номер

ЛО24-0017-00/0058053.0023.2022

ФГИС «Моя школа» соответствует всем нормативно-
правовым актам Российской Федерации, руководящим и
методическим документам ФСТЭК и ФСБ России,
регламентирующим вопросы защиты информации,
обрабатываемой во ФГИС «Моя школа».



МОЯ ШКОЛА



ГОСУСЛУГИ

Доступ к образовательному сервису может быть
осуществлен с помощью портала Госуслуг

**Благодарим
за внимание**



Обратная связь



Служба технической поддержки:

support@myschool.edu.ru

Горячая линия:

8 800 505-47-16

Форма обратной связи:

«Связаться с нами»

Информационный канал:

https://vk.com/myschool_edu