




Обеспечение информационной безопасности участников образовательного процесса при работе с сервисами цифровой образовательной среды



Государственная единая облачная платформа (ГЕОП)

Полный комплекс мер для информационной защиты инфраструктуры.
Сертифицированные средства защиты (соответствие техническим требованиям к безопасности информации)



Меры обеспечения информационной безопасности, применяемые на государственном уровне при создании компонентов цифровой образовательной среды

-  **Обеспечение конфиденциальности информации**
При создании ИС используется отечественное программное обеспечение (российские операционные системы, сертифицированные системы управления базами данных, средства защиты от несанкционированного доступа).
-  **Обеспечение целостности информации**
Организационные меры:
 - регламенты проведения обслуживания;
 - нормативно-правовые акты;
 - контроль за эксплуатацией информационной системы.Технические меры:
 - запись информации о действиях пользователя и ее отправка в базу данных для отслеживания действий с объектами в системе;
 - мониторинг событий информационной безопасности для выявления потенциальных угроз и аномалий;
 - регулярное резервное копирование на выделенное хранилище для обеспечения возможности восстановления в случае сбоев.
-  **Обеспечение санкционированного доступа**
 - Доступ в личный кабинет через Единую систему идентификации и аутентификации (ЕСИА);
 - Использование сертифицированных средств защиты для авторизации пользователей.

-  **Обеспечение доступности информации**
Компоненты в архитектуре ИС для обеспечения доступности:
 - средства противодействия кибератакам, направленным на отказ в обслуживании;
 - межсетевые экраны, которые осуществляют контроль, фильтрацию и блокировку запрещенного трафика, в том числе, межсетевые экраны уровня приложений;
 - системы обнаружения вторжений;
 - антивирусная защита.Кроме того, для снижения вероятности выхода из строя различных частей системы применяются отказоустойчивые схемы, обеспечивающие непрерывность работы.
-  **Защита пользователей от информации, причиняющей вред их здоровью**
 - Использование Единой сети передачи данных (ЕСПД) с использованием криптографических протоколов для защиты данных;
 - Контроль доступа в сети ЕСПД со стороны Минцифры и Минпросвещения

Меры обеспечения информационной безопасности, которые должны соблюдать учащиеся, учителя и родители

1. Используйте надежные пароли и постоянно их меняйте. Пароль должен быть сложным – не менее 12 символов, включая большие и маленькие буквы, цифры и специальные символы.
2. Храните пароли в надежном месте и не передавайте их никому, даже друзьям и коллегам. Используйте менеджер паролей.
3. Используйте антивирусное программное обеспечение.
4. Регулярно обновляйте программное обеспечение: операционные системы, веб и мобильные приложения.
5. Регулярно производите резервное копирование файлов.
6. Установите пароль на ноутбуке и мобильном телефоне.
7. Настройте многофакторную аутентификацию для всех основных учетных записей (электронная почта, социальные сети, банковские приложения).
8. Не переходите по подозрительным ссылкам в электронной почте, sms, и социальных сетях.
9. Не открывайте вложения с неизвестными или двойными расширениями (например: *.doc.exe, *.docx.js, *.bat).
10. Не размещайте персональные данные в социальных сетях.