

Актуальные вопросы информатизации образования Забайкальского края

Казакова Л.И., проректор, директор Центра информационных технологий и дистанционного обучения, ГУ ДПО «Институт развития образования Забайкальского края»



Единая система
идентификации
и аутентификации



Сетевой Город. Образование



Образовательная организация

Управление образования

Регион

Забайкальский край

Муниципальный район

Все

Город/село



Портал образовательных услуг Забайкальского Края

Поиск заявления/обращения по номеру

Регистрация обращения в общеобразовательную организацию в первый класс

Внимание! Услуга подачи обращения гарантированно работает в двух последних версиях браузеров Google Chrome, Firefox, Internet Explorer, Safari, Яндекс

Внимание!

Данные заполняются на основании информации из документов.

Проверочное слово использует кириллицу в любом регистре и цифры.

При входе через ЕСИА, для подтвержденных пользователей будут автоматически заполнены паспортные данные заявителя и адрес регистрации.

Чтобы перейти на следующий шаг, корректно заполните все поля, обозначенные «*». Данные, заполненные Вами, должны полностью совпадать с данными в документах, даже если поля не обозначены «*».

Указание не полных или ошибочных данных может являться основанием для аннулирования заявления образовательной организацией.

Вход с учетной записью Windows

Вход с учетной записью портала гос. услуг

Войти



«...дети с раннего возраста должны приобретать навык информационной безопасности. Основы кибербезопасности должны проговариваться в стандартах начального образования, в рамках программы воспитания и социализации, на уроках информатики, ОБЖ, обществознания и права. Мы дальше будем работать, прежде всего, по доработке дополнительных профессиональных программ для педагогических работников в области информационной безопасности...»

Васильева О.



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 2813

Выдан 15 января 2013 г.
Действителен до 15 января 2016 г.
Срок действия продлен до 15 января 2019 г.



Совет главных
конструкторов
информатизации
регионов РФ

www.pvti.ru
www.mininform.ru

fait@minsvyaz.ru
vniipvti@pvti.ru

тел: +7 (495) 771-8156
+7 (495) 235-5809

факс: +7 (495) 771-8788
+7 (495) 235-5267

№ _____
На № _____ от _____

ЗАКЛЮЧЕНИЕ

На основании результатов экспертизы прикладных информационных систем и решений, настоящим подтверждается, что перечисленные ниже прикладные информационные системы и решения могут быть рекомендованы для включения в число типовых программно-технических решений, внедряемых в регионы Российской Федерации.

В сфере образования:

1. АИС «Е-услуги. Образование», АИС «Сетевой город. Образование» (ЗАО «ИРТех», г. Самара);
2. ИС «БАРС.Web – Электронная Школа», ИС «БАРС.Web – Электронный Детский Сад» (ООО «БАРС Групп», г. Казань).

В сфере имущественно-земельного комплекса:

1. АИС «ТМ-Имущество» (ЗАО «ТНДМ Софт МСК» - дочернее общество ЗАО «Корпорация Галактика», г. Москва);

Приложение 1 Технические требования к Рабочему месту оператора в образовательном учреждении

Требования к программному обеспечению:

1. На рабочем месте должна быть установлена лицензионная операционная система из семейства Microsoft Windows (XP, 7, 8, 8.1)
2. Установлен один из браузеров: Google Chrome, Firefox, Internet Explorer, Яндекс.
3. Установлено сертифицированное по требованиям безопасности антивирусное средство. (Касперский Endpoint Security или Dr.Web).
4. Установлено сертифицированное по требованиям безопасности средство криптографической защиты информации и межсетевое экранирование VIPNet Client 4.x. Подключение VIPNet Client 4.x должно осуществляться к защищенной сети Института Развития образования Забайкальского края (номер сети VIPNet № 5244).

Требования к организационно-распорядительной документации

В образовательной организации должны быть разработаны и утверждены следующие организационно-распорядительные документы:

- 1) Техническое задание на создание системы защиты информации;
- 2) Модель угроз безопасности персональных данных;
- 3) Модель нарушителя;
- 4) Акт классификации ИСПДн;
- 5) Технический паспорт;
- 6) Политика информационной безопасности;
- 7) Положение о защите ПДн в ИСПДн;
- 8) Положение об обработке ПДн;
- 9) Описание технологического процесса обработки информации;
- 10) Порядок обработки обращений субъектов персональных данных;
- 11) Инструкция пользователя;
- 12) Журналы учёта.

А если ничего не предпринимать?

Ответственность предусмотрена:

УК РФ: ст. 137 (штраф до 200 тыс. руб.,
лишение свободы до 2х лет, лишение права
занимать определенную должность).

КоАП РФ: ст. 5.39, ст. 13.11, ст. 13.12, ст. 13.14
(штрафы до 20 тыс. руб.).

Кто проверит?

Федеральная служба безопасности
Российской Федерации (ФСБ).

Федеральная служба по надзору в сфере
связи, информационных технологий и
массовых коммуникаций (РОСКОМНАДЗОР).

Федеральная служба по техническому и
экспортному контролю (ФСТЭК РОССИИ).

Прокуратура (По заявлению).