РОССИЙСКАЯ КОМПАНИЯ-РАЗРАБОТЧИК КОМПЛЕКСНЫХ РЕШЕНИЙ IT-БЕЗОПАСНОСТИ «СМАРТ-СОФТ»

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

для самостоятельной работы сотрудников школы

Профессиональные дисциплины:
«Безопасный Интернет для детей»

ДОСТУП БЕЗ ОПАСНОСТИ

Как защитить школьную сеть от вредоносной информации
без ущерба для учебного процесса

Каждая пятая российская школа не способна защитить детей от информации, причиняющей вред их здоровью и развитию. Директора учебных заведений доверяют такой важный вопрос, как соблюдение закона при организации интернет-доступа, провайдеру. Между тем не все провайдеры способны отфильтровать запрещенные для школьников ресурсы. В результате родители не могут быть на 100% уверены, что в школе дети не попадут на страницы, просмотр которых дома запрещен.

ТОП-3

головных болей директора школы из-за Интернета

1. Первая и главная – **штрафы со стороны контролирующих ведомств** за то, что школа не смогла защититься от сетевых и информационных угроз. Администрации школ обязаны соблюдать Федеральные законы РФ: № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» по вопросу ограничения доступа к противоправной информации в сети Интернет. Это подразумевает блокировку ресурсов, не предназначенных для просмотра детьми. К ним относятся сайты, на которых пропагандируются наркотики, отрицаются семейные ценности, содержится нецензурная брань, информация порнографического характера, и другие ресурсы, указанные в законах, регламентирующих информационную безопасность детей.

2. **Излишне жесткая блокировка ресурсов,** из-за чего учителя и ученики иногда не могут выйти на полезные образовательные сайты и даже на собственный школьный. Чтобы открыть их для работы, администрация школы вынуждена обращаться к провайдеру с заявлением о внесении данного ресурса в список разрешенных.

3. **Падение локальной сети** из-за чрезмерной нагрузки на сеть Wi-Fi или, например, из-за функционирования необходимых по регламенту генераторов белого шума во время проведения ЕГЭ.

ТОП-3

страхов родителей, отправляющих детей на занятия

1. **Сайты, пропагандирующие экстремизм, наркотики** и прочие опасности, на которые могут попасть дети, подключившись к незапароленным точкам школьной сети Wi-Fi.

2. **Педофилы, маньяки, распространители наркотиков,** жертвами которых могут стать дети, находясь в социальных сетях без контроля со стороны взрослых.

3. **Компьютерные игры и переписка с одноклассниками,** которыми могут заниматься дети, вместо того чтобы слушать учителя.

ЧТО ДЕЛАТЬ?

Директорам – найти программное обеспечение, которое позволит выполнить все требования закона, чтобы не зависеть от провайдера.

Родителям – настаивать, чтобы администрация школы провела грамотную «интернетизацию» учебного заведения.

Компания «Смарт-Софт» выпустила специальную версию решения для школ **Traffic Inspector School Edition**, обеспечивающую комплексный безопасный доступ к сети Интернет в учебных заведениях.

В чем ее преимущества?

1. Продукт отвечает главному требованию – имеет лицензию и сертификат ФСТЭК и обладает техническими возможностями, позволяющими соблюдать законы РФ. Основной компонент системы безопасности и контроля – универсальный аппаратно-программный шлюз DEPO Traffic Inspector с программой FSTEC.

2. Модуль NetPolice обеспечивает гибкую контентную фильтрацию. С одной стороны, позволяет соблюсти федеральные законы о защите детей от

вредоносных ресурсов, а с другой – не блокирует все подряд, вынуждая администраторов сети каждый раз связываться с провайдером, чтобы внести конкретный ресурс в список разрешенных к просмотру.

3. Специальная версия обеспечивает разделение доступа для разных категорий пользователей: гостей школы, учеников, учителей и администрации. При такой системе школьники, даже если они одновременно выйдут в Сеть, не оставят директора без доступа в Интернет.

4. Специалисты компании, помимо обучения системного администратора и технического персонала работе с программным обеспечением, оказывают последующую техническую поддержку школам.

Таким образом, благодаря Traffic Inspector School Edition, при информатизации своих школ директора соблюдают законы, регулирующие интернет-доступ, и тем самым защищают себя от возможных санкций со стороны Роскомнадзора и других контролирующих органов. А родители могут быть совершенно уверены, что школьный Интернет не навредит их ребенку.

ВНИМАНИЕ! ДЛЯ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ ДЕЙСТВУЮТ СКИДКА 70% НА БЕЗЛИМИТНУЮ ВЕРСИЮ TRAFFIC INSPECTOR И СПЕЦИАЛЬНЫЕ ЦЕНЫ НА МОДУЛИ.

ВОСПОЛЬЗУЙТЕСЬ НОВЫМ ВЕБ-СЕРВИСОМ

для проверки школьной сети на соответствие законам

check.smart-soft.ru

ОПЫТ

Пример информатизации муниципального бюджетного общеобразовательного учреждения «Гимназия № 8», Коломна

Проблема	Решение
Несоблюдение ФЗ-436, ФЗ-139, ФЗ-152, ФЗ-149	Контентная фильтрация и соблюдение ФЗ-436, ФЗ-139, ФЗ-152, ФЗ-149
Нет возможности разграничения пользователей	Разграничение доступа пользователей
При сбоях в системе – индивидуальная настройка компьютеров	Централизованное управление с помощью удаленного доступа
Устаревшее серверное оборудование	Современный интернет-сервер для организации, защиты и контроля доступа в Интернет
Отсутствие доступа в Интернет	Доступ в Интернет при использовании генераторов белого шума

Инструкция для системного администратора по организации интернет-доступа в образовательном учреждении

С помощью данной инструкции вы сможете просто и быстро организовать безопасный Интернет в вашем учреждении.

Для организации с нуля или модернизации IT-инфраструктуры школы в соответствии с действующим законодательством: № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты РФ» по вопросу ограничения доступа к противоправной информации в сети Интернет необходимо выполнить все следующие пункты:

1. Подготовительные работы

На данном этапе необходимо произвести инвентаризацию имеющейся ИТ-инфраструктуры, разработать методологию систем маркировки, определить политику доступа к имеющимся службам и сервисам, учесть планируемые дополнительные сервисы.

По результатам инвентаризации появляется возможность судить о масштабе необходимой замены оборудования. При планировании закупок дополнительного оборудования рекомендуется придерживаться следующих советов:

а) со стороны СКС: по возможности использовать управляемые свитчи с гигабитными портами и поддержкой технологии VLAN. Установить коммутационные шкафы на все точки расположения свитчей, в случае их отсутствия использовать патч-панели для коммутации, рассчитать количество LAN-розеток под каждого пользователя плюс на каждый кабинет иметь резервные розетки, промаркировать сетевые кабели;

б) со стороны серверной части: обязательно наличие хорошо вентилируемого, безопасного помещения для организации в нем серверной. Минимальная серверная конфигурация должна включать в себя сервер шлюза, контроллер доменных служб и файловый сервер. Сервером шлюза будет

выступать решение DEPO Traffic Inspector, которое позволит организовать контроль доступа пользователей в сеть Интернет, а также соответствовать требованиям производительности и безопасности. Контроллер доменных служб необходим для гибкого управления инфраструктурой, разграничения прав пользователей, а также централизованного распространения требуемых политик безопасности. Файловый сервер рекомендуется для централизованного хранения пользовательских данных. Для доменных служб и файлового сервера рекомендуется использовать специализированные серверные решения или, в случаях ограниченного бюджета, обеспечить отказоустойчивость дисковой подсистемы RAID-массивом. Рекомендуется производить резервное копирование данных служб на отдельные NAS-сервера;

в) со стороны клиентов: убедиться, что установленные редакции поддерживают интеграцию в доменные службы Active Directory.

Соответственно, на данном этапе системный администратор должен определить текущие узкие места в IT-инфраструктуре школы, изучить текущие работающие сервисы локальной сети, разработать методологию для маркировки кабельных систем, для облегчения диагностики в случае проблем с СКС и согласовать бюджет в соответствии с требованиями и возможностями руководства.

2. Проектирование политик IT-инфраструктуры, установка и настройка служб

Во время составления плана политик системному администратору необходимо разработать такую иерархическую систему, которая позволит охватить максимальное количество сходных пользователей минимальным набором правил. Данный подход позволит минимизировать количество дальнейших правок в уже рабочую инфраструктуру и обеспечить гибкость управления средой. Затем следует произвести установку или миграцию требуемых служб. Дополнительную информацию и пошаговые руководства по службам Microsoft можно найти по адресу https://technet.microsoft.com/. Также на данном этапе создаются необходимые учетные записи пользователей, групповые политики, иерархия файлового хранилища и его ACL-списков. Рассмотрим пример установки контроллера домена и создания ACL для общего ресурса:

а) перед установкой роли контроллера домена необходимо настроить сетевой интерфейс целевого сервера, назначив ему статическую настройку ip, и указать единственный адрес DNS сервера как 127.0.0.1;

б) устанавливаем роль «Контроллер домена Active Directory»;

в) после установки роли, если целевой сервер версии Windows 2008R2, запускаем команду dcpromo, если 2012R2 – выбираем пункт «Повысить до контроллера домена» в меню задач консоли управления сервером;

г) в открывшемся мастере указываем, что производим установку нового леса, – указываем желаемое имя нового леса вида <любое имя>.local – режим функционирования домена и леса оставляем без изменений – на этапе мастера с указанием пароля для режима восстановления служб Active Directory вводим пароль, который будет использоваться для авторизации в режиме восстановления AD, на остальных шагах мастера значения по умолчанию оставляем без изменений. По завершении работы мастера потребуется перезагрузка;

д) на данном этапе переходим к созданию организационных подразделений, пользователей и групп. Для их создания необходимо перейти в оснастку «Active Directory пользователи и компьютеры» либо же в окне «выполнить» написать «dsa.msc». Этап создания организационных подразделений и групп является довольно ситуационным и, как ранее было сказано, ответственным моментом, где необходимо заранее продумать иерархическую структуру, учитывающую логику IT-процессов школы. В дальнейшем, для понимания базовых принципов, мы рассмотрим упрощенный пример, когда мы создаем одно организационное подразделение для хранения одного пользователя и группы. В появившейся оснастке консоли создадим организационное подразделение (в иерархическом списке нажимаем ПКМ на корне текущего домена – создать – подразделение – в появившемся окне указываем имя подразделения (например, «Персонал») и нажимаем кнопку ОК). Выбираем в иерархическом списке наше созданное подразделение, нажимаем на нем ПКМ – создать – пользователь – в появившемся окне указываем данные пользователя, его имя входа – далее – указываем пароль пользователя, снимаем галку «Требовать смену пароля при следующем входе в систему». По завершении работы мастера в нашем организационном подразделении будет находиться созданный пользователь. По аналогии создаем группу пользователей, где указываем ее имя, настройки группы в мастере оставляем без изменений. Добавим нашего пользователя в новосозданную группу. Используем двойное нажатие левой кнопки мыши на целевой группе, в открывшемся окне выбираем вкладку «члены групп» – добавить – дополнительно – в графе имя указываем имя пользователя (или оставляем пустым) – кнопка поиск – двойной щелчок левой кнопкой мыши на целевом пользователе – ОК – ОК. Таким образом, данная группа будет содержать целевого пользователя;

е) теперь дадим этой группе ACL для доступа на расшаренную папку на файловом сервере. Если файловый сервер еще не введен в домен, то вводим его через Панель управления – система – в разделе «имя компьютера, домена ...» выбираем изменить настройки – в открывшемся окне кнопка «изменить» – переключить радиокнопку в положение «Домена» и ввести имя

домена нашей сети. Нажать в окнах ОК и дождаться перезагрузки сервера. Теперь создаем на желаемом диске требуемую иерархию папок (в нашем случае будет одна папка share на диске D) – нажимаем ПКМ на созданной папке – вкладка «Доступ» – «Общий доступ» – добавляем в список нашу целевую группу и указываем необходимые разрешения (например, чтение-запись) и нажимаем кнопку «Поделиться». Теперь наша папка доступна по сети с заданными разрешениями.

3. Внедрение сетевого шлюза

Данная стадия включает в себя установку программно-аппаратного комплекса DEPO Traffic Inspector, импорт пользователей из базы Active Directory, создание групп, настройка правил сетевого экрана, правил ограничений для различных групп пользователей (например, учащихся и рабочего персонала). Для создания правил блокировки сайтов, указанных в государственном реестре для образовательных учреждений, необходимо произвести следующую последовательность действий:

а) в консоли администрирования, в иерархическом дереве Traffic Inspector перейти в ветку «Объекты» – «IP-сети» – «Действия» – «Добавить список». В открывшемся мастере, на стадии «Автозагрузка», ввести URL для загрузки http://list.smart-soft.ru/IP/zapretinfo_ip.txt и указать периодичность обновления с данного URL. Рекомендуемое значение – 1 раз в сутки в нерабочее время. Данный список будет включать IP-адреса запрещенных ресурсов;

б) в области URL-списки выбрать действия – «Добавить список». Появится окно мастера, аналогичное предыдущему. На вкладке «Автозагрузка» указать в поле «Загружать с URL» адрес http://list.smart-soft.ru/URL/zapretinfo_url.txt. Данный список будет включать URL-адреса запрещенных ресурсов. Рекомендации по периодичности обновления – те же;

в) в разделе «Правила» – «Правила пользователей» иерархического списка консоли управления Traffic Inspector создать 2 запрещающих правила (в разделе мастера «Тип правила» – «Запрет»): одно с типом трафика «Любой» и указанием в разделе «IP адрес» – «Использовать список» – выбрать имя созданного списка в пункте а) и второе – с типом трафика «Трафик через прокси-сервер» с указанием в разделе «Проверка URL» – «Список» выбрать имя созданного списка в пункте б). Далее необходимо сделать привязку данных правил к целевой группе учащихся, через меню настроек, пункт «Правила группы до».

Детальный видеоурок по данному вопросу можно найти по адресу https://youtu.be/haGcleBtAI8.

Для более гибкой фильтрации возможно использование модуля контентной

фильтрации Netpolice, который предназначен для категоризации сайтов и создания соответствующих правил для блокировки по критерию категории, настраиваемой в разделе создания правила «Анализ контента» – пункт «Проверка категории контента».

В случае возникновения проблем вы можете обратиться в службу технической поддержки

+7 (495) 77-55-991

support@smart-soft.ru

форум компании «Смарт-Софт»
forum.smart-soft.ru

4. Настройка резервного копирования

Необходимо создать планы резервного копирования для каждого критического сервиса локальной сети либо же критически важных данных. Для доменных служб, в случае единственного контроллера домена, необходимо настроить полное резервное копирование и его периодичность (в зависимости от частоты правок базы Active Directory). Рекомендуется периодически проверять резервные копии на корректность.

5. Документация

Документация необходима для понимания IT-инфраструктуры школы. Поможет в быстрой адаптации новых сотрудников, ответственных за ИТ. В документацию рекомендуется внести схему текущей сети, используемое оборудование, описание схемы используемых политик, расписания резервного копирования и другие данные, которые позволят за короткое время вникнуть в IT-инфраструктуру.

КОММЕНТАРИИ

Хотим отметить следующие достоинства работы данного проекта компании «Смарт-Софт»: бесперебойная работа локальной вычислительной сети в гимназии, блокировка нежелательных сайтов, безопасная работа в Сети всех учащихся и сотрудников, удобство пользования и настройки продуктов. За время реализации безопасного доступа в Интернет учащимся гимназии № 8 команда специалистов проекта Traffic Inspector шла навстречу и тесно взаимодействовала с нашими сотрудниками. В гимназии были устранены все существовавшие проблемы с безопасной работой локальной вычислительной сети. Рекомендуем продукты компании «Смарт-Софт» к использованию в образовательных учреждениях и желаем новых успешных проектов.

С. В. Соколов,
директор МБОУ «Гимназия № 8»,
Московская область, Коломна

Мы непрерывно используем решение Traffic Inspector в нашем образовательном учреждении на протяжении 7 лет. За это время значительно выросли требования к IT-инфраструктуре, ее защищенности и соответствию федеральному законодательству. Благодаря наличию интуитивно понятного интерфейса в сочетании с глубоко продуманной функциональностью продукта мы неоднократно рекомендовали к использованию данное ПО коллегам из нескольких образовательных учреждений.

В. А. Ковалева,
директор МБОУ «Талажская средняя образовательная школа»,
Архангельская область, п. Талаги

Благодаря высокому уровню вашего профессионализма нам совместно удается выполнять такую важную миссию – обеспечивать успешное безопасное развитие и обучение подрастающего поколения!

А. В. Добран,
директор МБОУ СОШ № 32
Красноярский край, Норильск

ИНТЕРНЕТ И ЗАКОНОДАТЕЛЬСТВО

Законы РФ, регламентирующие правила и стандарты подключения к сети Интернет образовательных учреждений

- № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
- № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».
- № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- № 152-ФЗ «О защите персональных данных».
- Постановление Правительства РФ от 31 июля 2014 г. N 758 «Об идентификации пользователей Wi-Fi».

Аксиомы безопасности при работе в Интернете от РОЦИТ (Региональная общественная организация «Центр интернет-технологий»)

1. Не сохраняйте на своем компьютере неизвестные файлы, не переходите по ссылкам от незнакомцев, какими бы заманчивыми они ни были.

Такая ссылка может оказаться вирусом, трояном или, если «повезет», рекламой порносайта. 80% ссылок, получаемых от незнакомцев, являются рекламой, а 20% вредоносными объектами.

2. Обязательно установите антивирус и файервол и регулярно обновляйте их базы.

Необновленные и устаревшие базы не смогут гарантировать вам стопроцентную защиту от вредоносных объектов. Дело в том, что ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу необходимо как можно чаще получать информацию о методах борьбы с ними.

3. Не запускайте неизвестные файлы, особенно с расширением *.exe

Файл с таким расширением не может являться картинкой или фильмом. Это всегда программа, в крайнем случае флешка. Поэтому велика вероятность, что такой файл является вирусом или трояном.

4. Старайтесь давать как можно меньше информации о себе в Интернете. Ибо в Интернете вы рискуете стать объектом киберпреследования, мошен-

ничества или запугивания как для настоящих преступников, так и просто для любителей «пошутить». 90% случаев мошенничества происходит из-за утечки информации по вине пользователя.

5. Будьте осторожны при общении с незнакомыми людьми, они могут оказаться не теми, за кого себя выдают.

Ничто не мешает сорокалетнему извращенцу прикидываться в чатах пятнадцатилетней школьницей и заводить знакомства со «сверстницами». Опросы показывают, что каждый пятый пользователь Сети выдавал себя за другого человека (реально существующего или придуманного).

6. Поступайте и пишите в Сети так, как поступили/сказали бы в реальной жизни и как хотели бы, чтобы поступали с вами. Помните – все, что вы сделаете в Интернете, будет иметь последствия в реальной жизни.

Анонимность в Интернете не гарантирует, что любые поступки сойдут с рук. Вычислить человека по его виртуальным следам (IP, cookies, мак-адрес) не так уж сложно.

7. Уважайте своих собеседников и чужую собственность в Интернете, за ними скрываются настоящие люди и реальный труд.

У всех материалов, находящихся в Сети, есть авторы и хозяева.

Основные правила безопасности для социальных сетей (подходящие юзерам любого возраста) таковы:

– не следует «френдить» всех подряд. Дружить в социальных сетях нужно только с проверенными «в реале» друзьями;

– ни в коем случае нельзя публиковать в социальной сети то, что может обидеть и унизить других пользователей или просто других людей! Даже в шутку – такие «шутки» плохо кончаются;

– очень рекомендуется проверять антивирусом все присылаемые приложения;

– крайне не рекомендуется играть в социальной сети на деньги и запускать приложения, требующие денег за участие или поднятие в них своего «статуса»;

– если пользователь стал жертвой оскорблений или опасного контента, он может обратиться за помощью к администратору социальной сети или на горячую линию.

ПОЛЕЗНЫЕ РЕСУРСЫ

HTTP://PEDSOVET.SU/

СООБЩЕСТВО ВЗАИМОПОМОЩИ УЧИТЕЛЕЙ

На портале можно найти нашу статью о том, как защитить школьную сеть от вредоносной информации без ущерба для учебного процесса: http://pedsovet.su/publ/44-1-0-5942.

HTTP://HOTLINE.FRIENDLYRUNET.RU/?L=RU

ГОРЯЧАЯ ЛИНИЯ ЛИГИ БЕЗОПАСНОГО ИНТЕРНЕТА

Горячая линия принимает сообщения о распространении в Сети интернет-материалов с порнографическими изображениями несовершеннолетних.

Обратиться сюда можно по телефону: +7 (499) 685-01-85, по электронной почте: info@FriendlyRunet.ru или через сайт.

HTTP://CHECK.SMART-SOFT.RU/

ВЕБ-СЕРВИС ПО ПРОВЕРКЕ НА СООТВЕТСТВИЕ ЗАКОНАМ

Чтобы избежать проверок правоохранительных органов, контролирующих организацию интернет-доступа в заведении, узнайте, нарушаете ли вы закон, прямо сейчас. Достаточно пройти по ссылке и через бесплатный веб-сервис попробовать открыть запрещенные ресурсы. Тем, кто предоставляет бесплатный доступ к Сети, – просто необходимо.

HTTP://DETIONLINE.COM/HELPLINE/ABOUT

ЛИНИЯ ПОМОЩИ «ДЕТИ ОНЛАЙН»

Бесплатная всероссийская служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи. Обращения принимаются по бесплатному телефону: 8 (800) 25-000-15 или через форму обратной связи на сайте HTTP://WWW.HOTLINE.ROCIT.RU/

ГОРЯЧАЯ ЛИНИЯ РОЦИТ (РЕГИОНАЛЬНАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ «ЦЕНТР ИНТЕРНЕТ-ТЕХНОЛОГИЙ»)

На горячую линию можно сообщить о контенте, который, по вашему мнению, нарушает российское законодательство, а также о проблемах, связанных с предоставлением тех или иных услуг в Интернете (нелегальные/противоправные материалы, мошенничество, проблемы с интернет-сервисом – интернет-банкинг, интернет-магазин и пр.), низким качеством интернет-услуг.

HTTP://MEL.FM/

ИНТЕРНЕТ-ИЗДАНИЕ «МЕЛ»

Об образовании и обо всем, что его окружает, человеческим языком.

HTTP://BANKPORTFOLIO.RU/

ИНТЕРНЕТ-ПОРТФОЛИО УЧИТЕЛЕЙ

Банк интернет-портфолио учителей. Международный проект.

HTTP://NEWVIRUS.KASPERSKY.RU/

ГОРЯЧАЯ ЛИНИЯ ЛАБОРАТОРИИ КАСПЕРСКОГО

Лаборатория Касперского традиционно занимается фактами распространения в Сети компьютерных вирусов. Обратиться в лабораторию за помощью вы можете как в электронном виде (по электронной почте: cert@kaspersky.com или через сайт), так и по бесплатному телефону: +7 (800) 700-88-11.

HTTP://ROSPOTREBNADZOR.RU/

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА (РОСПОТРЕБНАДЗОР)

Как видно из названия, Роспотребнадзор выполняет функции по защите прав потребителей, а это значит, что обращаться сюда можно в случаях нарушения ваших прав со стороны российских интернет-магазинов. Прием обращений осуществляется в электронном виде.

Всероссийская программа поддержки социальных инициатив детей и молодежи

Тетрадка Дружбы

О ПРОГРАММЕ «ТЕТРАДКА ДРУЖБЫ»

История создания. Авторы

Программа «Тетрадка Дружбы» придумана в 2006 году. Автор – Ольга Викторовна Зубкова, педагог, международный эксперт культурных программ Организации Объединенных Наций, автор более 100 педагогических разработок по вовлечению детей и молодежи в социально значимые формы деятельности, генеральный директор АНО «Вектор Дружбы». Соавторами программы выступили школьники Пермского края, придумав компоненты технологии в формате «дети для детей». Поскольку в разработке программы участвовали дети, ее механизм прост и гениален в своей простоте. На сегодняшний день в программе участвуют более 1200 образовательных учреждений из 40 регионов России.

Актуальность программы

Еще совсем недавно родители могли с уверенностью доверить школе воспитание своих детей. До начала 90-х школы России, гармонично сочетая обучение и воспитание, проводили системную работу по формированию разносторонне развитых и социально ответственных граждан страны. Однако после упразднения пионерии и комсомолии в качестве альтернативных полноценных государственных воспитательных программ, способных на долгий срок прижиться в школах, ничего предложено не было. В результате сформировалось целое поколение молодых людей, многие из которых замкнуты в своем внутреннем (зачастую виртуальном) мире, с низким уровнем общей культуры, с коммуникативными проблемами, с претензией на быстрые и нетрудоемкие результаты.

Пока взрослые думали, что сочинить взамен канувших в лету «идеологических» воспитательных программ, дети придумали способ объединения школьников независимо от возраста, успеваемости, социального статуса родителей, физических характеристик, географии проживания, национальности. Программа «Тетрадка Дружбы» стала уникальной технологией для безграничного позитивного общения, детских социально-значимых инициатив и творчества, в дополнение к учебному процессу.

Главный атрибут программы

Что может стать объединяющим атрибутом для взаимодействия всех детей в мире? То, что привычно, понятно и одинаково доступно всем детям. Таким атрибутом стала обычная школьная тетрадь. Простая ученическая тетрадка с логотипом и специальным дизайном, превратившись в «Тетрадку Дружбы», сегодня выполняет функцию объединяющего атрибута для школьников образовательных учреждений из 40 регионов России, заменив пионерский галстук и комсомольский значок. Специальные тетради как обязательный элемент участия в детской долгосрочной программе выступают «пропуском» в мир разнообразных тематических мероприятий длиною в учебный год.

Роль «Тетрадки Дружбы» в реализации программы

Все дети разные, поэтому подход к участникам программы индивидуальный, и тетрадки можно применить по-разному. Неуверенным в себе, закомплексованным, безынициативным ребятам предлагается рабочий вариант «Тетрадки Дружбы» просто для того, чтобы стать участником, членом большой команды детской социокультурной программы. Такие дети используют «Тетрадки Дружбы» на уроках как обычные рабочие тетради (по русскому языку, математике, физике и пр.) Однако педагоги замечают, что именно в «Тетрадках Дружбы» у ребят меняется почерк, появляется ответственность в выполнении домашнего задания, нет желания вырвать листы, неопрятно вести записи, появляется заинтересованность в том, что будет дальше с этими тетрадками.

Ребята, которые хотят выразить свои таланты и способности на страницах тетрадки, могут использовать «Тетрадки Дружбы» в качестве творческих тетрадей. Участники программы могут написать на страницах конкурсных тетрадей свои стихи и рассказы, описать социальные проекты и культурные туристические маршруты по малой родине, рассказать о традициях семейных чтений и пр. Часто к заполнению тематических тетрадей подключаются педагоги и родители. Таким образом, «Тетрадка Дружбы» становится универсальным средством самовыражения, коммуникации, творчества, диалога ровесников и людей разных поколений.

Также для творческой реализации участников программы, для возможности общаться «в живом режиме» детям, педагогам, родителям из разных школ, городов, регионов России каждый месяц проходят разноформатные интерактивные мероприятия. Годовой цикл мероприятий позволяет создавать атмосферу постоянного живого творческого общения участников. Совместная деятельность детей, родителей и педагогов в процессе подготовки к мероприятиям создает условия для эффективного взаимодействия институтов семьи и школы, делая их соучастниками социокультурных инициатив. Системная занятость участников программы в творческих, спортивных, добровольческих практиках решает проблемы профилактики негативных явлений, формирует в школах страны добровольческие отряды, службы примирения, патриотические клубы.

Знаковые события в истории развития программы

15 октября 2014 года в рамках форума ОНФ «Качественное образование во имя страны» президент России Владимир Путин отметил актуальность Всероссийской культурно-образовательной программы «Тетрадка Дружбы» и высказался в поддержку распространения «Тетрадок Дружбы» во всех школах России.

Программа получила широкое признание на международном уровне. «Тетрадка Дружбы» признана одной из лучших сетевых практик на конференциях в ООН «Добровольчество – технология социальных преобразований (Женева, 2010–2015 гг.). Программа вошла в шестерку лучших социальных проектов на Международном форуме в поддержку Всемирного дня НКО (Хельсинки, 2014 г.). Генеральный секретарь ООН Пан Ги Мун лично познакомился с «Тетрадкой Дружбы» в рамках сессии ЭКОСОС молодежного форума «Год возможностей для молодежи» (Нью Йорк, 2015).

Перспективы

На сегодняшний день идет процесс регистрации Детско-молодежной общероссийской общественной организации «Тетрадка Дружбы». Готовится к открытию новый сайт программы. Пока с подробностями инновационной технологии можно познакомиться на сайте http://www.тетрадкадружбы.рф/. Для всех, кто заинтересован в присоединении к новой организации, актуальная информация здесь: http://тетрадка-дружбы.рф/.

О КОМПАНИИ

Партнеры

2 500 ПАРТНЕРОВ

Более 2 500 партнеров на российском и международном рынках

Пользователи

4 500 000 ЧЕЛОВЕК

4 500 000 человек работают в сетях, где установлены наши решения

Уверенность в завтрашнем дне

13 ЛЕТ

13 лет на рынке информационной безопасности

КОНТАКТЫ

Звоните: +7 (495) 77-55-991
Пишите: info@smart-soft.ru
www.smart-soft.ru