КИБЕРБЕЗОПАСНОСТЬ

для учеников и родителей QSIB

В современной школе информация, информационная инфраструктура – один из главных компонентов учебного процесса.

Проблема информационной безопасности образовательного учреждения, школьников в ней – одна из самых актуальных на современном этапе.

Общими мерами по созданию безопасной информационной системы в школе являются:

- Защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, атаки хакеров и т. д.)
- Использование контентной фильтрации Интернета, для фильтрации сайтов с одержимым, далёким от задач образования.
- Обучение детей основам информационной безопасности, воспитание информационной культуры.

Защита компьютеров и других устройств на территории школы

Использование Антивирусного программного обеспечения

На всех школьных компьютерах установлена ESET NOD32 Smart Security Business Edition которая включает в себя:

- Расширенную защиту рабочих станций, с усиленной функцией файервола, веб-контроля и антиспама.

- Функция безопасного браузера для дополнительной защиты данных от перехвата

- Высокий уровень защиты файловых серверов без снижения производительности

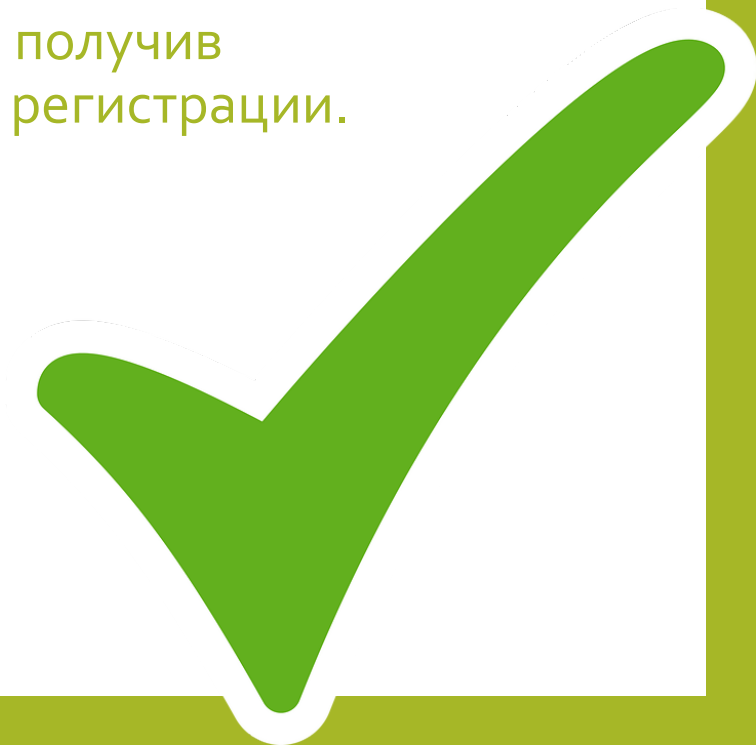
- Инструменты централизованного управления продуктами и лицензи

- Обнаружение сложных угроз

Регистрация девайсов в школьной сети

- Все компьютеры и телефоны получают доступ к сети только после прохождения регистрации в специальной программе администрирования.

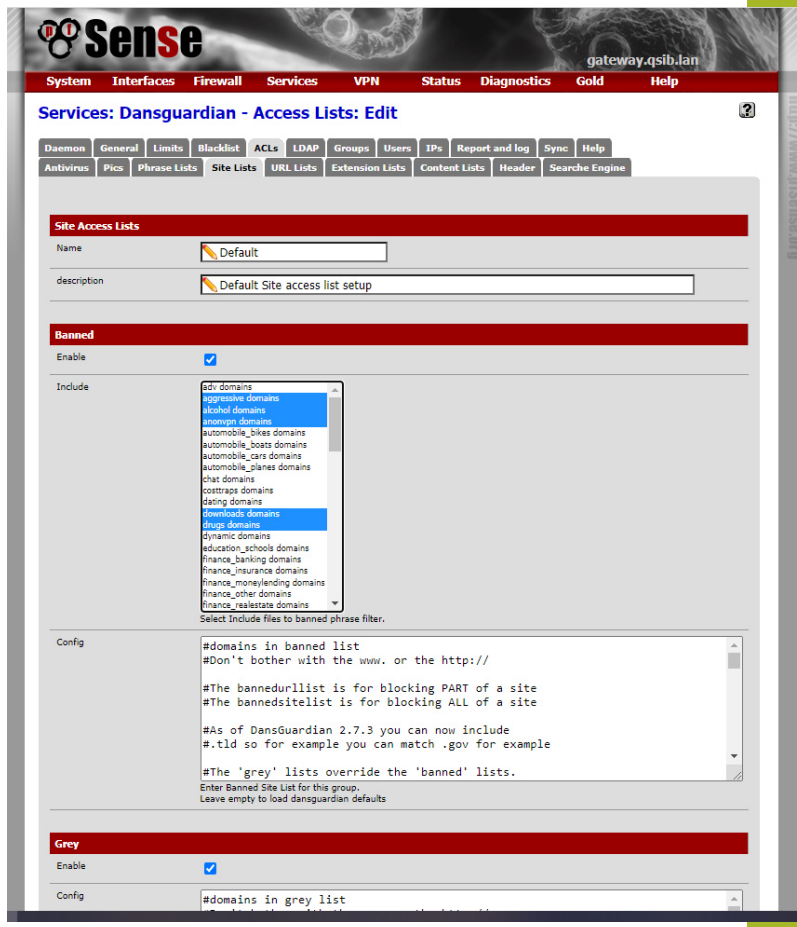
- Воспользоваться услугами сети интернет возможно только получив разрешение школьного системного администратора после регистрации.



DANS GUARDIAN – Контент-фильтр

- Все компьютеры и телефоны, подключенные к школьной сети автоматически включены в систему фильтрации контента Dans Guardian. Это продукт, разработанный специально для образовательных учреждений QSI. При его создании учитываются реалии интернет-пространства и особенности построения сетевой инфраструктуры в образовательных учреждениях.
- Фильтрация происходит как по содержимому сайта, так и по категориям. Есть особо строгий режим "белого списка", когда блокируется доступ ко всем ресурсам, кроме одобренного перечня. В нем по умолчанию сайты образовательных ресурсов, учреждений, порталов (но его можно настраивать).

- Dans Guardian предотвращает доступ хакеров в компьютерную сеть, взлом и кражу данных, установку на компьютеры вирусов, скриптов слежения и другого вредоносного ПО.
- Производит антивирусную проверку контента.
- Блокирует не только контент, предусмотренный законом, но и сайты, мешающие образовательному процессу: социальные сети, блоги, форумы, Youtube и т.п. (администрация школы сама может настроить правила блокировки).
- Блокирует рекламу - баннеры, видео, всплывающие окна - так как она способна содержать недопустимую информацию (сам сайт при этом может находиться в "белом" списке). К тому же, без рекламы web-страницы загружаются быстрее.
- Ограничивает трафик на компьютерах, которые потребляют его слишком много, поэтому интернет не тормозит, даже если в школе слабый канал.



Уроки Информационной Безопасности

Для Родителей:

- Ознакомительная беседа с родителями проводится в начале каждого учебного года.

- Подготовка памятки о Кибербезопасности для взрослых и детей.

- Обсуждение основных тактик по детской интернет-безопасности.

- Подписание Acceptable Use Policy (Договор о школьной кибер безопасности)

Общие правила для родителей

- Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
- Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
- Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, сайты взрослого содержания, интернет казино, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
- Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
- Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.
- Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Десять правил безопасности для детей в Интернете*

1. Посещайте сеть вместе с детьми, поощряйте их делиться опытом использования Интернета
2. Научите детей доверять интуиции - если их в Интернете что-либо беспокоит, пусть сообщают вам
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты
4. Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки
5. Объясните детям, что в Интернете и реальной жизни разница между правильным и неправильным одинакова

6. Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают
7. Скажите детям, что далеко не все, что они читают или видят в Интернете, - правда, приучите их спрашивать вас, если они не уверены
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает

9. Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире

Уроки Информационной Безопасности для детей

- Подробное изучение Digital Citizenship (уроки цифрового гражданства) на уроках информатики
- Разработка стратегии действий детей в случае небезопасного использования интернета.
- Регулярные беседы о кибер безопасности на уроках ОБЖ.

Памятка о интернет-безопасности для детей

- Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
- Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
- Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься, и номер твоего телефона должны знать только родители и друзья.
- Никогда не отправляй свои фотографии людям, которых не знаешь лично. Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.
- Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
- Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
- Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.

Правила безопасности в Интернете

Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому, где работают твои родители и номера их телефонов.

Всегда спрашивай родителей о непонятных вещах, которые ты встречаешь в Интернете. Они расскажут тебе, что можно делать, а что нет.

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения — сразу скажи об этом родителям!

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс — не делай этого! Ты можешь потерять деньги, которые мог бы потратить на что-то другое.

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Помни, что твой пароль можешь знать только ты и твои родители.

SkyDNS

Глоссарий

- **Антивирусная программа -** Программа, предназначенная для предотвращения доступа к персональному компьютеру для вредоносных программ — она обнаруживает инфицированные файлы и удаляет их.
- **Брандмауэр** - Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.
- **Вирус** - Вредоносная программа, которая распространяется, копируя себя в другие программы. Вирус может распространяться через файлы, сообщения электронной почты или веб-страницы. Компьютер может заразиться вирусом во время работы пользователя в Интернете или при открытии вложений электронной почты. Вирусы могут снизить работоспособность компьютера или системы.
- **Всплывающее окно -** Новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит собственного веб-адреса, однако в некоторых случаях может его содержать. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклама.

- **Дискуссионный форум** - Место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация.
- **Загрузка** -Сохранение файлов из Интернета на собственном компьютере.
- **Защита данных** - Набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.
- **Информационная безопасность-** Политика, реализуемая для обеспечения контроля над рисками информационной безопасности.
- **Операционная система -** Главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся Microsoft® Windows®, Apple® Mac OS и Linux®.

- **Опасные программы: вирусы, черви и трояны**
  Программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, вирусов, червей или троянов.
- **Почта; электронная почта; сообщение электронной почты -**
  Электронная передача текста или изображений между адресами компьютерного приложения.
- **Сервер** - Программа, которая распределяет файлы по компьютерам в сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты сети. Сервером часто называют компьютер, на котором установлена серверная программа.
- **Сетевой дневник -** Общественный интерактивный дневник.
- **Спам -** Нежелательная электронная почта, которая, как правило, рассылается в целях прямого почтового маркетинга. Спам почти всегда единовременно рассылается большому кругу получателей.

- **Хакер, взломщик -** Человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. Примечание: термин «хакер» имеет два значения — он может также означать опытного компьютерного пользователя. (см. Хакеры и взломщики)
- **Чат -**Дискуссионный форум, работающий в режиме реального времени. В нем пользователи поочередно пишут сообщения, сразу отображающиеся на экране. Сообщения заменяются по мере написания новых, поэтому отображаются только самые последние сообщения.
- **Червь** - Вредоносная программа, которая может независимо распространяться через информационные сети. Черви могут распространяться через электронную почту или бреши в системе защиты информации в обозревателе Интернета или операционной системе. Даже если пользователем не выполняются никакие действия, черви могут получить доступ к незащищенным компьютерам при их подключении к Интернету. Черви затрудняют работу системы или компьютера и могут распространять другие вредоносные программы.