**Организация работы по обеспечению безопасности в сети интернет**

1. **Ответственность**

В целях осуществления ограничения доступа наших обучающихся к вредной информации в сети Интернет был разработан приказ 31 августа 2021 года. В приказе был ряд обязательных требований, которые школа взялась выполнить для решения данной цели. Первым из них было назначено лицо, ответственное за организацию доступа к сети Интернет в Рыбинской школе-интернат №1 – Иванова Анастасия Александровна.

Далее работа уже двигалась с большим рядом документации, согласно приказу, выполнялись активные действия по решению поставленных задач. Об этом чуть позже.

1. **Закон РФ об информационной безопасности в школе.**

Сейчас хочется рассказать в связи с чем были приняты эти меры.

Федеральные законы: «Об образовании в Российской Федерации»

«О противодействии экстремистской деятельности»

«О защите детей от информации, причиняющей вред их здоровью и развитию»

«Об информации, информационных технологиях и о защите информации»

«Об основных гарантиях прав ребенка в Российской Федерации»

«О рекламе»

«О персональных данных»

«О безопасности»

Указы Президента РФ: «О Стратегии национальной безопасности Российской Федерации»

«Об утверждении Доктрины информационной безопасности Российской Федерации»

Приказ Минкомсвязи России «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»

Приказ Федеральной службы по надзору в сфере образования и науки "Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информации"

**Все приказы в полном объеме можно найти и ознакомиться на сайте школы в разделе «Информационная безопасность»**

1. **Раздел Безопасный интернет - Центр телекоммуникации**

Так же, на сайте школы можно найти ссылку на очень полезный Областной информационно-образовательный портал. Он может сильно помочь в работе и соблюдении всех законов. В разделе «Безопасный интернет» можно найти тему «Педагогам». Там множество материалов и для проведения уроков, занятий, и для просветительской работы с родителями и тд.

К примеру, «Азбука цифрового мира» содержит в себе видео, игры и темы, доступные для наших детей. Даже присутствует материал, оформленный в виде комикса, чтобы детям было интересней воспринимать скучную информацию.

1. **Нормативные акты**

Теперь вернемся к нашей работе по безопасности в сети Интернет.

Наши были разработаны нормативные акты по данному направлению.

Их полные формулировки вы можете видеть на слайде. Я кратко озвучу:

* Положение об ограничении доступа обучающихся (воспитанников) к Интернету.
* Инструкция о порядке действий сотрудников.
* Правила использования сети Интернет сотрудниками.
* План мероприятий по обеспечению информационной безопасности обучающихся.
* Должностная инструкция лица, ответственного за организацию доступа к сети (т.е. моя)
* Документ по внедрению системы контентной фильтрации.
* Формулировки для внесения дополнений в должностные инструкции работников.

1. **План 21-24**

Из перечня всех документов хочется подчеркнуть один очень важный.

План мероприятий по обеспечению информационной безопасности обучающихся.

**Этот план рассчитан на 2021-2024 года и состоит** из 20ти пунктов.

**В каждом пункте** указаны сроки выполнения и ответственные лица.

* Изучение нормативно - правовой базы
* Заключение договора с оператором связи
* Настройка (установка) технических средств
* Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации
* Ознакомление работников образовательной организации с методическими рекомендациями
* Ознакомление работников образовательной организации с сайтами в сети «Интернет», включенных в Реестр безопасных образовательных сайтов
* Информирование работников образовательной организации, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации
* Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети Интернет, о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей
* Проведение периодического контроля состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет
* Организация проведения уроков (классных часов) для обучающихся по основам информационной безопасности
* Проведение Единого урока по безопасности в сети «Интернет» Проведение серии мероприятий проекта «Сетевичок» для обучающихся
* Организация участия педагогических работников в дистанционной конференции по формированию детского информационного пространства «Сетевичок»
* Ведение локальных нормативных актов образовательной организации в области информационной безопасности обучающихся
* Оформление и обновление стенда «Информационная безопасность»
* Размещение на официальном сайте образовательной организации информации по вопросам обеспечения информационной безопасности детей
* Прохождения педагогическими и иными работниками образовательной организации программы повышения квалификации на сайте Единыйурок.рф по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации».

(На слайде вы видите фамилии педагогов, которые этот пункт плана уже выполнили)

* Участие сотрудников образовательной организации в работе Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества в сфере образования и воспитания.
* Участие обучающихся, родителей (законных представителей) обучающихся и сотрудников образовательной организации в деятельности Межрегионального детского движения в области обеспечения безопасности и развития детей в информационном пространстве «Страна молодых»
* Использование в работе образовательных программ, направленных на формирование навыков у обучающихся, их родителей и педагогических работников безопасного поведения в информационной среде

1. **Информация о компьютерах и пользователях**

Всего компьютеров и иных аналогичных устройств 48. Под «иными устройствами» подразумеваются интерактивные панели разных моделей. Из них 43 устройства подключены к сети Интернет. Из этих 43 устройств 20 используются в учебно-образовательном процессе.

1. **Провайдер**

Провайдер (компания, обеспечивающая нас интернетом) – Ростелеком. Этот провайдер для нас бесплатный.

1. **Роскомнадзор**

Если есть законы, то существуют и службы, которые будут следить за исполнением этих законов. Такой контрольной организацией является Роскомнадзор.

Нашу школу может коснуться проверка этой службы. Нарушение какого-либо пункта приказа или несоответствие нормативного документа закону, является Административным правонарушением. Естественно, это означает штраф учебному заведению.

1. **Контрольная документация**

Для избежания подобной неприятности, к нашим нормативным документам мы добавили ряд контрольных документов. Это ряд журналов учета и проверок. По порядку познакомим вас с ними:

* «Журнал контроля контентной фильтрации». Этот документ ведет ответственное лицо (т.е. я). Один или несколько раз за четверть проводится проверка любого интернет-носимого устройства. В случае обнаружения «вредного» сайта или проблемы со скоростью интернета, об этом указывается в таблице в соответствующей графе.

В заполненном варианте таблицы видно, что за весь период ведения документа, проблем не обнаружено.

* «Журнал регистрации случаев обнаружения сайтов». Раз проблем не было обнаружено, этот документ остается чистым.
* График работы точки доступа к сети Интернет. Здесь указано в какой период работает интернет в школе.
* Акт установки системы контентной фильтрации. Это большой документ с полным перечнем всех компьютеров и аналогичных устройств с интернетом или без. Указаны имена, должности, место работы, инвентарные номера устройств, пароли от всех компьютеров.
* Акт проверки контентной фильтрации. Этот документ заполняется 2 раза в год. Его подписывает целый ряд ответственных лиц.
* «Журнал учета доступа в сеть Интернет». Самый популярный и часто используемый нами документ в прошлом учебном году. Так он выглядел. Каждую четверть пользователи интернетом сдавали ответственному лицу (т.е. мне) этот документ.

Так он выглядит в заполненном виде *(слайд).* Кто-то заполнял его каждый день, у некоторых за четверть набиралось несколько целиком исписанных листов, за кем-то приходилось «бегать» и просить сдать документ. Этих листов было всё больше, и больше с каждой четверть. И в конечном итоге накопилось очень много.

В итоге мы поняли насколько такой формат неудобен и разработали два новых документа. В одном перечень работников, использующих интернет, цель использования. Во втором находится указывается график работы пользователей интернетом. Оба документа заполняет ответственное лицо (т.е. я). Всё что здесь необходимо от остальных – устное подтверждение, что интернет в этот промежуток времени использовался, и только с целью работы.

Такой формат намного упростил нам всем жизнь.

1. **Базовые требования соблюдения информационной безопасности на рабочих местах**

**Доступ к ресурсам и сервисам, обеспечивающим функции образовательной организации**

1. **Используйте только сложные пароли:** они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры. Если пароль простой, злоумышленник удаленно с помощью специальных программ сможет подобрать его простым перебором.
2. **Пароли должны быть уникальными:** не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать в этом случае доступ ко всем ресурсам.
3. **Пароли должны быть секретными:** не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами. Иначе случайный посетитель или уволившийся сотрудник сможет воспользоваться таким паролем.
4. **Если сервис позволяет включить** [**двухфакторную аутентификацию**](https://www.kaspersky.ru/blog/2fa-notification-trap/21282/)**, включите ее.** Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

**О важности персональных данных**

1. **Не передавайте файлы с персональными данными по электронной почте или по открытым каналам** (например, через Google Docs по прямой ссылке или через публичные файлохранилища).
2. **Не делитесь персональными данными, к которым Вы по своим обязанностям имеете доступ,** с коллегами, чьи рабочие функции не требуют такого доступа, с посторонними лицами, с обучающимися.

**О самых распространенных киберугрозах**

1. **Тщательно проверяйте ссылки в письмах, прежде чем по ним переходить.** Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут попробовать подсунуть фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег.
2. **Убедитесь, что на всех рабочих компьютерах подключена автоматическая проверка антивирусом при подключении USB устройств** (флеш-накопители, карты памяти, переносные жесткие диски, телефоны сотрудников через USB) . При настройке антивируса установите отключение автозапуска любой информации с подключаемых через USB устройств. Не подключайте к рабочему компьютеру любые сторонние флеш носители.
3. **Не открывайте и не запускайте любые файлы из непроверенного источника** (например, присланные по почте). При открытии файла всегда нужно смотреть, не является ли он исполняемым (злоумышленники часто маскируют вредоносные файлы под офисные документы). Любой присланный по почте файл необходимо сначала сохранить в папку, выделенную на локальном компьютере для файлов, которые не проверены антивирусом, затем, не открывая его, запустить проверку на вирусы в этом файле.

На этом у меня всё. Приятной и безопасной работы в сети интернет!