**План**

***обеспечения безопасности образовательного учреждения при подготовке***

***и проведении массовых мероприятий***

**СОДЕРЖАНИЕ**

1. Введение\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_3
2. Практические мероприятия по предотвращению актов терроризма и чрезвычайных ситуаций в образовательном учреждении и на его территории\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_5
3. Пример Комплексного плана подготовки и проведения в

образовательном учреждении массовых мероприятий, посвящённых

празднованию Новогодних и других праздников\_\_\_\_\_\_\_\_\_8

1. Заключение\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_23
2. Литература\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 24

**ВВЕДЕНИЕ**

Тема проекта очень актуальна в настоящее время, т.к. обеспечение безопасности учащихся и сотрудников – это основная задача администрации любого образовательного учреждения. Особенно сейчас, когда этот вопрос встаёт особенно остро. Теперь, в период активности террористических организаций, экстремистских действий и, конечно же, в период участившихся случаев бандитизма, хулиганства и неадекватных поступков как среди детей, так и среди взрослых, мы должны особенно серьёзно относиться к обеспечению безопасности образовательного учреждения.

Особенно большое внимание мы должны уделять безопасности во время подготовки и проведения массовых мероприятий, которых всегда бывает очень много в любой школе. И именно во время этих мероприятий и случаются, как правило, все чрезвычайные происшествия.

План обеспечения безопасности образовательного учреждения при проведении массовых мероприятий составляется не позднее, чем за месяц до проведения мероприятия, и утверждается лицом, ответственным за безопасность ОУ (заместителем директора (по безопасности)), и лицом, ответственным за проведение массового мероприятия (заместителем директора по ВР). Утверждается руководителем образовательного учреждения.

При проведении любых массовых мероприятий пост охраны усиливается сотрудниками ОВД и администрацией школы. С учетом нахождения образовательной организации в очагах межнациональной и социальной напряженности, возникает необходимость и целесообразность увеличения числа сотрудников охраны на данный период минимально до трех человек, для осуществления возможности быстрого реагирования на внештатную ситуацию.

Перед тем, как начать подготовку к проведению массового мероприятия в образовательном учреждении, необходимо определить те цели и задачи, которые следует решать. В данном случае нас интересует обеспечение безопасности учащихся и сотрудников образовательного учреждения во время проведения мероприятия.

Обеспечение безопасности, в свою очередь, подразумевает, прежде всего, недопущение возникновения чрезвычайных ситуаций и террористических актов во время проведения массового мероприятия в образовательном учреждении.

Для того, чтобы обеспечить безопасность во время проведения массового мероприятия, администрация образовательного учреждения должна разработать и выполнить Комплексный план подготовки и проведения в образовательном учреждении массового мероприятия.

Возникает вопрос, почему это план «комплексный»? Потому, что все мероприятия по обеспечению безопасности мы должны выполнить в комплексе, ни в коем случае не разделяя антитеррористическую безопасность от пожарной, информационную от эпидемиологической и т.д. Только тогда, когда будет обеспечена комплексная безопасность, можно будет сказать, что учащиеся и сотрудники образовательного учреждения находятся в полной безопасности и их жизням ничто не угрожает.

**ПРАКТИЧЕСКИЕ МЕРОПРИЯТИЯ**

**ПО ПРЕДОТВРАЩЕНИЮ АКТОВ ТЕРРОРИЗМА И ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ И НА ЕГО ТЕРРИТОРИИ**

В образовательном учреждении перед поведением массового мероприятия и во время его проведения необходимо предпринимать усиленные меры безопасности по предотвращению диверсионно-террористических актов:

***1***. Заместителю директора школы по административно-хозяйственной части (АХЧ) содержать в порядке подвальные и подсобные помещения, выходы на крышу и запасные выходы из здания учреждения, которые должны быть закрыты и опечатаны. Опечатаны должны быть также огнетушители и электрощиты. Ежедневно осуществлять контроль за состоянием этих объектов. Следить за освещением территории ОУ в темное время суток.

***2.*** Заместителю директора по учебно-воспитательной работе не реже одного раза в неделю проверять состояние учебных помещений (классов, кабинетов, учебных мастерских, музея, библиотеки, спортивного и актового залов). Контролировать выдачу ключей от учебных помещений педагогам и сдачу ключей по окончанию занятий и наведения порядка в учебных помещениях. Осуществлять контроль за работой дежурных педагогов.

***3.*** Постоянному составу школы прибывать на свои рабочие места за 10-15 минут до начала занятий с целью проверки их состояния на предмет отсутствия посторонних и подозрительных предметов и подготовки их к занятиям (работе).

***4.*** Педагогам, проводящим занятия в незакрепленных за ними учебных помещениях (классах, кабинетах и др.), расписываться в получении и сдачи ключей от них в специальной книге. Контролировать уборку учебного помещения после окончания занятий.

***5.*** Обучающимся пребывать в образовательное учреждение заблаговременно с целью своевременной подготовки к началу занятий. При входе учащиеся школы предъявляют охраннику пропуск (дневник, паспорт безопасности) в развернутом виде. Постоянный состав пропускается по списку, утвержденному директором образовательного учреждения при предъявлении документа, удостоверяющего личность (паспорт).

***6.*** Дежурному педагогу и обучающимся дежурного класса своевременно, за 30 минут, прибывать на свои рабочие места и готовить их к работе (знакомиться с инструкцией, выявлять посторонние и подозрительные предметы).

***7.*** Заместителю руководителя (по безопасности) и уполномоченному на решение задач в учреждения ежегодно планировать и проводить командно-штабные учения с руководящим составом учреждения и должностными лицами ; тренировки со всем личным составом образовательного учреждения по действиям при возникновении угрозы совершения террористического акта в помещениях и на территории образовательного учреждения. Готовить и представлять директору -начальнику учреждения - предложения по приобретению средств индивидуальной защиты (СИЗ), приборов химической и радиационной защиты, видео и компьютерной техники и учебных материалов к ней, учебно-методической литературы и наглядных пособий по вопросам противодействия терроризму и обеспечения безопасности обучающихся и сотрудников.

***8.*** Дежурному педагогу:

-инструктировать учащихся дежурной группы;

- не пропускать в помещения учреждения обучающихся и сотрудников с подозрительной ручной кладью (тяжелые сумки, ящики, большие свертки и т.д.);

- составлять списки сотрудников и обучающихся несвоевременно пребывающих на работу и занятия и представлять их заместителю директора по УВР для принятия соответствующих мер;

***9.*** Дежурному сторож:

- пропускать в здание образовательного учреждения сотрудников по списку, утвержденному директором образовательного учреждения при предъявлении документа, удостоверяющего личность (паспорт), учащихся по их паспортам безопасности и дневникам;

- при пропуске на территорию образовательного учреждения автотранспортных средств, проверять соответствующие документы и характер ввозимых грузов;

- особое внимание уделять проверке документов и цели прибытия лиц из других организаций, посещающих образовательное учреждение по служебным делам, делать соответствующие записи в книге посетителей;

- ограничить пропуск в здание школы родственников и знакомых обучающихся (пропускать только с разрешения руководителей администрации, учителей, классных руководителей);

- держать входные двери здания свободными для входа и выхода во время массового прибытия сотрудников и обучающихся. В остальное время суток входные двери должны находиться в запертом состоянии и открываться охранником по звонку посетителя;

- после окончания рабочего дня регулярно обходить и проверять внутренние помещения образовательного учреждения и каждые два часа обходить прилегающую к учреждению территорию, обращать внимание на посторонние и подозрительные предметы;

- обеспечить своевременный вывоз мусора с территории учреждения;

- обо всех обнаруженных нарушениях немедленно докладывать руководителю учреждения или его заместителю по обеспечению безопасности и своим непосредственным начальникам в охранном предприятии.

***10.*** Каждый сотрудник и обучающийся образовательного учреждения обязан при обнаружении недостатков и нарушений, касающихся обеспечения безопасности в учреждении, незамедлительно сообщить об этом руководителю образовательного учреждения или его заместителю по обеспечению безопасности.

**ПРИМЕР КОМПЛЕКСНОГО ПЛАНА ПОДГОТОВКИ И ПРОВЕДЕНИЯ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ МАССОВЫХ МЕРОПРИЯТИЙ**

Утверждаю

Директор МКОУ НСОШ им.Х.И.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Баяджиева З.А.

«01» 09. 2021г.

***Комплексный план***

***по подготовке и проведению массовых***

***мероприятий***

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки | Ответственный |
|  | **I. РАБОТА С КАДРАМИ** |  |  |
| 1 | Распределение обязанностей в работе по созданию безопасных условий труда и предупреждению детского травматизма между членами администрации и педколлектива | До 05.09 | Директор |
| 2 | Продолжение изучения с педколлективом школы «Положения о службе охраны труда в системе Министерства образования РФ» и других нормативных актов | В течение года | Директор, заместитель директора |
| 3 | Обучение членов трудового коллектива, вновь принимаемых на работу, | В течение года | Директор, заместитель директора |
| 4 | Проведение регулярных инструктажей персонала школы по вопросам охраны труда с регистрацией в соответствующих журналах | В течение года | Директор, заместитель директора |
| 5 | Проведение оперативных совещаний по вопросам состояния охраны труда в ОУ | На планёрках | Директор, заместитель директора |
|  | **II. РАБОТА С УЧАЩИМИСЯ** |  |  |
| 1 | Проведение повторных инструктажей в 1-4, 5-9 классах (на начало учебного года) с регистрацией в журнале | До 18.09 | Классные руководители, ответственный за охрану труда среди учащихся |
| 2 | Проведение вводных инструктажей в 1–9 классах (на начало учебного года) | 02.09 | Классные руководители, ответственный за охрану труда среди учащихся |
| 3 | Проведение инструктажей при организации учебных занятий по спец. предметам (вводных, на рабочем месте, повторных, внеплановых, целевых) | Сентябрь  В течение года | Зам. директора по УВР, зав. кабинетами |
| 4 | Проведение тематических инструктажей в 1–9 классах в рамках классных часов:  - по правилам пожарной безопасности;  - по правилам электробезопасности;  - по правилам дорожно-транспортной безопасности;  - по правилам антитеррористической защищенности.  - по правилам безопасности на воде и на льду;  - по правилам безопасности на спортивной площадке;  **-** по правилам безопасности при обнаружении взрывчатых веществ и подозрительных предметов;  - о поведении в экстремальных ситуациях;  **-**по правилам безопасного поведения на железной дороге;  **-** по правилам поведения во время каникул. | По планам классных руководителей | Классные руководители, учитель ОБЖ |
| 5 | Проведение внеплановых инструктажей при организации внеклассных мероприятий | В течение года | Заместитель по УВР, классные руководители |
| 6 | Проведение целевых инструктажей при организации трудовой деятельности учащихся | В течение года | Классные руководители,  ответственный за охрану труда среди учащихся, учителя предметники. |
| 7 | Проведение внеплановых инструктажей по вопросам состояния детского травматизма в школе, районе, городе. | В течение года | Классные руководители |
| 8 | Проведение профилактических бесед работников ГИБДД, пожарной части с учащимися | 1раз в год | Педагог-организатор |
|  | **III. РАБОТА С РОДИТЕЛЯМИ** |  |  |
| 1 | Изучение с родителями вопросов обеспечения безопасности школьников в рамках педагогического всеобуча по темам:  ? предупреждение дорожно-транспортного травматизма детей;  ? соблюдение правил пожарной безопасности;  ? безопасное поведение на воде и на льду;  ? правила безопасности при обнаружении взрывчатых веществ и подозрительных предметов;  ? правила поведения в экстремальных ситуациях;  ? правила поведения учащихся в период каникул | По плану | Директор, классные руководители |

**2. Делопроизводство по охране труда**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки | Ответственный |
| 1 | Обновление инструкций по охране труда для учащихся и работников школы | В течение года | Директор, зав. кабинетами |
| 2 | Продолжение работы над пакетом локальных актов и документации по охране труда | В течение года | Директор, заместитель директора, пред. ПК |
| 3 | Составление актов проверки выполнения соглашения по охране труда | До 31.12 и до 30.06 | Директор, пред. ПК |

**3. Создание безопасных условий труда**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки | Ответственный |
| 1 | Проверка учебных кабинетов на предмет соответствия требованиям техники безопасности, проверка наличия и правильности заполнения журналов инструктажей | Август, январь | Директор, заместитель директора , пред. ПК |
| 2 | Переоснащение школы новыми огнетушителями и перезарядка имеющихся | До 1.09 | Директор, завхоз |

**4. Обеспечение безопасности учащихся на дорогах**

|  |  |  |  |
| --- | --- | --- | --- |
| **№/№** | **Название мероприятий** | **Сроки** | **Ответственные** |
| 1. | Составление плана работы школы по профилактике детского дорожно-транспортного травматизма | Август | Учитель ОБЖ |
| 2. | Неделя безопасности по дорожному движению. | сентябрь | Классные руководители |
| 3. | Конкурс рисунков «Грамотный пешеход» | 1 раз в четверть | Учитель ОБЖ |
| 4. | Родительские собрания: безопасного поведения детей на улицах и дорогах города; вопрос детского травматизма | 2 четверть | Классные руководители, инспектор ГИБДД |
| 5. | Инструктаж на классных часах по ПДД, по правилам поведения на улицах и дорогах города, в общественных местах | 1 раз в месяц | Классные руководители |
| 6. | Проведение дней профилактики ДДТТ «Внимание! Дорога! Пешеход!» | В течение учебного года | классные руководители |
| 7. | Проведение тематических утренников, викторин, игр, конкурсов, соревнований с участием ГИБДД и родителей:  - 1-2 классы – утренник «Волшебная палочка»;  3-4 классы – викторина «Осторожно! Перекрёсток!»;  5-9 классы – конкурс «Дорога в школу и домой». | В течение учебного года | Классные руководители |
| 8. | Обновление уголка ЮИД | В течение учебного года | Учитель ОБЖ |
| 9. | Встречи с учащимися 1-9 классов с инспектором ГИБДД | В течение учебного года | классные руководители |
| 10. | Проведение уроков безопасности «Мой безопасный путь домой» | В течение учебного года | Классные руководители |
| 11. | Распространение буклетов «Памятка школьнику: безопасная жизнь в твоих руках!» | 2 раз в полугодие | классные руководители |
| 12. | Агитбригада «Знай правила движения как таблицу умножения» | Февраль | Учитель ОБЖ |
| 13. | Беседа «Уверенные действия по оказанию первой помощи» | В течение учебного года | классные руководители |
| 14. | Турнир юных пропагандистов | В течение учебного года |  |
| 15. | Конкурс на лучший плакат «Безопасная дорога» | 1 раз в четверть | Классные руководители |
| 16. | Классные часы по теме: «Безопасное движение на улицах и дорогах города», «Светофор», «Как разговаривает улица», «Осторожно! Перекрёсток!» | 1 раз в четверть | Классные руководители |

**5. Обеспечение курса ОБЖ**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки | Ответственный |
| 1 | Проведение практических занятий по ОБЖ с учащимися | В течение года | Учитель ОБЖ, классные руководители |
| 2 | Проведение уроков ОБЖ и тематических классных часов | В течение года | Учитель ОБЖ, классные руководители |
| 3 | Проведение бесед классными руководителями с детьми перед выходом на внешкольные мероприятия, перед началом трудовой практики и в канун каникул с записью в журнале инструктажей | В течение года | Классные руководители, ответственный за охрану труда среди учащихся |

**6. Мероприятия по предупреждению  
террористических актов**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки | Ответственный |
| 1 | Инструктажи педперсонала и учащихся по темам:  ? действия по предупреждению установки взрывчатых веществ;  ? действия при обнаружении подозрительных предметов;  ? о порядке действий при получении анонимных сообщений с угрозами совершения актов терроризма | В течение года | Директор, преподаватель ОБЖ,  классные руководители |
| 2 | Установка поста охраны в школе | До 1.09 | Директор |
| 3 | Ежедневная проверка и опечатывание подсобных помещений, чердаков | В течение года | Заведующий хозяйством |
| 4 | Регулярная проверка помещений | В течение года | Администрация |
| 5 | Отработка практических действий по эвакуации персонала школы и учащихся по сигналу тревоги | 1 раз в четверть | Директор, классные руководители |
| 6 | Обследование территории и прилегающих помещений во время проведения массовых мероприятий с учащимися | В течение года | Директор, завхоз |
| 7 | Наблюдение за автотранспортом, находящимся в пределах зоны безопасности школы. | В течение года | Директор, заместители  дежурные учителя |
| 8 | Оповещение педколлектива, учащихся и родителей об экстренных телефонах | До 5.09 | Директор, классные руководители |

**7. Мероприятия по противопожарной безопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование мероприятий | Срок выполнен | Ответственный за выполнение |
| 1 | Обновление инструкции по правилам пожарной безопасности и планов эвакуации с порядком действий при пожаре | В течение года | Директор |
| 2 | Оформление противопожарного уголка в коридоре | В течение года | Директор |
| 3 | Изучение с работниками школы Правил пожарной безопасности | 1 раз в год | Директор, преп.-орг. ОБЖ |
| 4 | Проведение с обучающимися бесед и занятий по правилам пожарной безопасности согласно программе | 1 раз в четверть | Преп.-орг. ОБЖ, клас. рук. |
| 5 | Проведение с обучающимися инструктажа по правилам пожарной безопасности с регистрацией в специальном журнале | Сентябрь  январь | Классные руководители |
| 6 | Организация инструктажей по правилам пожарной безопасности со всеми работниками школы с регистрацией в специальном журнале | Октябрь | Директор |
| 7 | Проведение практических занятий с обучающимися и работниками школы по отработке плана эвакуации в случае возникновения пожара | Сентябрь.  Апрель | Директор, заместители  преп.-орг. ОБЖ |
| 8 | Проведение проверки сопротивления изоляции электросети и заземления оборудования с составлением протокола | Август | завхоз |
| 9 | Проведение перезарядки огнетушителей, а также контрольное взвешивание порошковых огнетушителей. Занесение номеров огнетушителей в журнал учета первичных средств пожаротушения | Июнь-август | завхоз |
| 10 | Оборудование запасных выходов из здания школы легко открывающимися запорами и обозначение их светящимися табло от сети аварийного освещения и указательными знаками | В течение года | завхоз |
| 11 | Проверка исправности электроустановок, электровыключателей, наличия в электрощитах стандартных предохранителей и отсутствия оголенных проводов | В течение года | завхоз |
| 12 | Обеспечение соблюдения правил пожарной безопасности при проведении детских утренников, вечеров, новогодних праздников, других массовых мероприятий, установка во время их проведения обязательного дежурства работников | В течение года | Зам. директора по УВР, педагог-организатор, клас. рук. |
| 13 | Разработка системы оповещения при пожаре | Август | Директор |
| 14 | Систематическая очистка территории школы от мусора, недопущение его сжигания на территории | постоянно | Администрация |

**ЗАКЛЮЧЕНИЕ**

Я привела пример Комплексного плана по подготовке и проведению массовых мероприятий , постаралась показать, насколько большая и трудоёмкая работа ведётся в школе для того, чтобы обеспечить безопасность. В эту работу вовлекаются абсолютно все члены школьного коллектива.

В случае необходимости администрация школы может обращаться в органы ОМВД для получения помощи полиции в обеспечении безопасности во время проведения массовых мероприятий. Правоохранительные органы могут разрабатывать свои планы по обеспечению безопасности массовых мероприятий и доводить их до сведения руководства образовательного учреждения. В этом случае план по обеспечению безопасности образовательного учреждения при подготовке и проведении массового мероприятия составляется с учетом планов органов внутренних дел.

При подготовке к проведению массовых мероприятий и перед непосредственным их проведением учебные и осмотровые мероприятия отражаются в текущих документах по безопасности: инструктажи – в журнале инструктажей; тренировки – в журнале тренировочных эвакуаций; проверки – в журнале «Об оперативной обстановке и принятых мерах».

В каждом образовательном учреждении есть свои нюансы, своя система работы по обеспечению безопасности. Но основные моменты этой работы у всех одинаковые, т.к. все образовательные учреждения имеют примерно одинаковые проблемы в обеспечении безопасности и сталкиваются в своей работе со схожими ситуациями и вопросами, которые приходится решать ежедневно, быстро и безболезненно для всех учащихся и сотрудников школы.

**ЛИТЕРАТУРА**

1. Н.В.Андреева, Х.М.Асеев, В.И.Беляев, А.И.Котова, Л.Я.Олиференко, В.Ф.Пилипенко, В.Ф.Сауткин, Т.И.Шульга «Обеспечение комплексной безопасности в образовательном учреждении (настольная книга руководителя)», «Айрис Пресс, Айрис Дидактика», Москва, 2005г.
2. Б.В.Вилков, М.А.Гаврилов, Б.В.Коваленко, А.И.Котова, Л.Я.Олиференко, В.Ф.Пилипенко, В.Ф.Сауткин «Комплексная безопасность образовательного учреждения (рабочий журнал заместителя руководителя по безопасности), ИПК и ПРНО МО, Москва, 2005г.
3. Петров С. В. Концепция безопасности образовательного учреждения. // ОБЖ. Основы безопасности жизни. № 10. 2004.
4. В.А. Акимов. Безопасность жизнедеятельности. Безопасность в чрезвычайных ситуациях природного и техногенного характера: Учебное пособие / В.А. Акимов, Ю.Л. Воробьев, М.И. Фалеев и др. Издание 2-е, переработанное — М.: Высшая школа, 2007.
5. Человеческий фактор в обеспечении безопасности и охраны труда: Учебное пособие / П.П. Кукин, Н.Л. Пономарев, В.М. Попов, Н.И. Сердюк.— М.: Высшая школа, 2008.

Памятка для обучающихся об информационной безопасности детей

Нельзя

* 1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
  2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
  3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;
  4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
  5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

Осторожно

* 1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
  2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
  3. Незаконное копирование файлов в Интернете - воровство;
  4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
  5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

Можно

* 1. Уважай других пользователей;
  2. Пользуешься Интернет-источником - делай ссылку на него;
  3. Открывай только те ссылки, в которых уверен;
  4. Обращаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут

Информационная памятка для обучающихся для размещения на официальных интернет-ресурсах

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

* 1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
  2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
  3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
  4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
  5. Ограничь физический доступ к компьютеру для посторонних лиц;
  6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
  7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

* 1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
  2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
  3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
  4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
  5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";
  6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

* 1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
  2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
  3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
  4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
  5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
  6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
  7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

* 1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
  2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
  3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;
  4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

* 1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
  2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный\_фанат@" или "рок2013" вместо "тема13";
  3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
  4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
  5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
  6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
  7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
  8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

* 1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
  2. Управляй своей киберрепутацией;
  3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
  4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
  5. Соблюдай свою виртуальную честь смолоду;
  6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
  7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
  8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

* 1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
  2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
  3. Необходимо обновлять операционную систему твоего смартфона;
  4. Используй антивирусные программы для мобильных телефонов;
  5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
  6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
  7. Периодически проверяй, какие платные услуги активированы на твоем номере;
  8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
  9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

* 1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
  2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
  3. Не указывай личную информацию в профайле игры;
  4. Уважай других участников по игре;
  5. Не устанавливай неофициальные патчи и моды;
  6. Используй сложные и разные пароли;
  7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

* 1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
  2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
  3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
  4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
  5. Установи надежный пароль (PIN) на мобильный телефон;
  6. Отключи сохранение пароля в браузере;
  7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

* 1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
  2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
  3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.