

критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

4). **Медиаобразование** - выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества.

**2. Основные задачи и функции должностных лиц,**

**ответственных за информационную безопасность обучающихся и сотрудников**

2.1. Основными задачами должностных лиц, ответственных за информационную безопасность, являются:

1). организация эффективной эксплуатации и текущий контроль технических и программных средств защиты информации;

2). организация и контроль резервного копирования информации;

3). защита обучающихся от любых видов пропаганды, рекламы, запрещенной законом информации.

4). формирование навыков медиаграмотности у всех участников образовательной деятельности.

2.2. Должностные лица администрации ОУ ответственные за информационную безопасность, выполняют следующие основные функции:

1). соблюдают инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в системе Интернет;

2). при наличии производственной необходимости организуют обучение персонала и пользователей навыкам работы с персональным компьютером (далее - ПК), правилам безопасной обработки информации и правилам работы со средствами защиты информации;

3). осуществляют антивирусный контроль магнитных носителей информации и файлов электронной почты, поступающих в ОУ;

4). осуществляют текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;

5). осуществляют контроль целостности эксплуатируемого ПК программного обеспечения с целью выявления несанкционированных изменений в нём;

6). осуществляют контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;

7). осуществляют контроль за формированием: медиатеки в соответствии с основной образовательной программой дошкольного образования ОУ; развивающих интерактивных игр;

8). осуществляют контроль пользования сетью Интернет;

9). осуществляют контроль доступа к официальному сайту, к официальной электронной почте, деловой почте, официальной странице VK, к электронным базам данных.

2.3. Должностные педагогические лица ОУ (в соответствии с профессиональным стандартом «Педагог»):

1). участвуют в создании безопасной и психологически комфортной информационной среды как составляющей образовательной среды ОУ;

2). участвуют в планировании и корректировке соответствующих организационных и образовательных задач в сотрудничестве с другими участниками образовательных отношений; 3). обеспечивают информационную безопасность детей;

4). планируют и реализуют образовательную деятельность по формированию культуры безопасности, предпосылок информационной культуры в соответствии с федеральным государственным образовательным стандартом дошкольного образования;

5). оценивают безопасность информационной среды ОУ;

6). развивают профессионально значимые компетенций, необходимые для обеспечения информационной безопасности детей.

2.4. Должностные педагогические лица ОУ должны уметь:

1). анализировать объекты информационной среды ОУ, выявлять потенциальные угрозы; 2). выбирать информацию, печатную и аудиовизуальную продукцию, соответствующую возрастным особенностям, интересам и потребностям детей;

3). на элементарном уровне осуществлять экспертизу информационной продукции для детей; 4). выбирать и применять наиболее эффективные методы формирования культуры безопасности, предпосылок становления информационной культуры в разные возрастные периоды в соответствии с индивидуальными особенностями детей;

5). выстраивать партнерское взаимодействие с родителями (законными представителями) детей в вопросах обеспечения информационной безопасности воспитанников.

2.5 Должностные педагогические лица ОУ должны знать «Концепции информационной безопасности детей»:

1). Соответствие информационной нагрузки возрастным и индивидуальным особенностям детей.

2). Возможности для развития мировосприятия детей, формирования позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке, психологическое благополучие.

3). Потенциал для ценностного, морального, нравственно-этического развития.

4). Трансляция системы семейных ценностей и представлений о семье.

5). Условия для развития системы социальных и межличностных отношений и общения.

6). Возможности для удовлетворения и развития познавательных потребностей и интересов, любознательности, исследовательской активности.

7). Ресурсы для когнитивного развития.

8). Потенциал для развития творческих способностей.

9). Возможности для формирования толерантности, установок толерантного сознания и поведения.

10). Содействие развитию личности, Я-концепции, социальной (гражданской, этнической, гендерной) и личностной идентичности.

11). Поддержание эмоционально-личностного развития и позитивного эмоционального состояния.

12). Отсутствие контента, вызывающего риски десоциализации, развития и закрепления девиантного и противоправного поведения, включая такие формы как: агрессивное поведение и применение насилия, жестокости по отношению к людям и животным; совершение действий, представляющих угрозу жизни и (или) здоровью ребенка, в том числе причинение вреда своему здоровью; употребление наркотических средств, психотропных и (или одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на их основе; противоправное поведение и (или) преступления

**3. Использование сети Интернет в образовательном учреждении**

3.1. В ОУ используются только сайты в сети «Интернет», включенные в Реестр безопасных образовательных сайтов. Использование сайтов в сети «Интернет», не включенных в Реестр безопасных образовательных сайтов, запрещается.

3.2. Контроль за использованием сотрудниками сети Интернет осуществляют должностные лица ответственные за информационную безопасность;

- во время проведения образовательной деятельности контроль использования сети Интернет осуществляет заведующий или заместитель заведующего ОУ;

- образовательная деятельность с использованием ИКТ осуществляется через флеш-носитель.

3.3. Обучающимся в сеть Интернет самостоятельный доступ не предоставляется.

3.4. Педагогическим работникам и сотрудникам ОУ запрещается:

1). обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают требованиям, установленным для сайтов Реестра безопасных образовательных сайтов;

2). осуществлять любые сделки через Интернет;

3). осуществлять загрузки файлов на компьютер ОУ без специального разрешения.

3.5. При обнаружении ресурса, содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, педагогические работники и сотрудники ОУ обязаны незамедлительно сообщить об этом заведующему или заместителю заведующего. Педагогический работник, самостоятельно выявивший ресурс, содержащий информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.

3.6. Должностные лица, ответственные за информационную безопасность при поступлении сообщения обязаны: принять информацию и направить информацию о выявлении ресурса оператору Реестра безопасных образовательных сайтов в течение суток. Передаваемая информация должна содержать: доменный адрес ресурса; сообщение о тематике ресурса; дату и время обнаружения; информацию об установленных в ОУ технических средствах технического ограничения доступа к информации.

**4. Информационная продукция, запрещенная для распространения среди детей**

Всем сотрудникам ОУ соблюдать меры по защите обучающихся от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение.

4.1. Классификация информационной продукции осуществляется по следующим категориям:

Законом установлено 5 категорий информационной продукции:

1). «0+» - информационная продукция для детей, не достигших возраста шести лет.

2). «6+» - информационная продукция для детей, достигших возраста шести лет.

3). «12+» - информационная продукция для детей, достигших возраста двенадцати лет.

4). «16+» - информационная продукция для детей, достигших возраста шестнадцати лет.

5). «18+» - информация, запрещённая к распространению среди детей.

4.2. **Информационная продукция, запрещенная для распространения среди детей**

К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные её жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

1). Побуждающая к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2). способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3). обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4). отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

4.1). пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения;

4.2). пропагандирующая педофилию;

4.3). способная вызвать у детей желание сменить пол;

5). оправдывающая противоправное поведение;

6). содержащая нецензурную брань;

7). содержащая информацию порнографического характера.

8). о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего;

9) содержащаяся в информационной продукции, произведенной иностранным агентом.

4.3. **Информационная продукция для детей, достигших возраста шести лет (6+)**

К допускаемой к обороту информационной продукции для детей, достигших возраста шести лет, может быть отнесена информационная продукция, предусмотренная статьей 7 настоящего Федерального закона, а также информационная продукция, содержащая оправданные её жанром и (или) сюжетом:

1). кратковременные и ненатуралистические изображение или описание [заболеваний](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B1%D0%BE%D0%BB%D0%B5%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого [достоинства](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D0%BE%D0%B8%D0%BD%D1%81%D1%82%D0%B2%D0%BE);

2). ненатуралистические изображение или описание аварии, [несчастного случая, [катастрофы](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%82%D0%B0%D1%81%D1%82%D1%80%D0%BE%D1%84%D0%B0),](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D1%87%D0%B0%D1%81%D1%82%D0%BD%D1%8B%D0%B9_%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9)  либо [ненасильственной смерти](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BD%D0%B0%D1%81%D0%B8%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%BC%D0%B5%D1%80%D1%82%D1%8C) без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;

3). не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

5. Обязанности и компетентность должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

5.1. Контролировать содержание и художественное оформление печатных изданий, полиграфической продукции, аудиовизуальной продукции, иной информационной продукции, используемой в образовательном и воспитательном процессе требованиям, предъявляемым к информационной продукции для детей соответствующей возрастной группы.

5.2. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать заведующему дошкольным учреждением о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений, принимать меры по восстановлению работоспособности средств и систем защиты информации.

5.3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

5.4. Создавать и удалять учетные записи пользователей.

5.5. Администрировать работу официального сайта ОУ (далее - сайт), размещать и классифицировать информацию на сайте.

5.6. Устанавливать по согласованию с заведующим критерии доступа пользователей на сайт, к электронным базам официальных документов, к официальной электронной почте ОУ.

5.7. При наличии производственной необходимости формировать и предоставлять пароли для новых пользователей, администрировать права пользователей сайта, электронных баз официальных документов ОУ, электронной почты ОУ.

5.8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку ПК на наличие вирусов.

5.9. Регулярно выполнять резервное копирование данных на сайте, в электронных базах официальных документов ОУ, при необходимости восстанавливать потерянные или поврежденные данные.

5.10. Систематически проверять информацию, поступающую по официальной электронной почте ОУ, официальный сайт ОУ.

5.11. Вести учет пользователей сетью Интернет. В случае необходимости лимитировать время работы пользователей в сети Интернет и объём скачиваемой информации.

5.12. Компетенции должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников

|  |  |  |  |
| --- | --- | --- | --- |
| № | Должность | Доступ к информационным средствам | Доступ к информации |
| 1 | Заведующий, заместитель заведующего | - электронные базы официальных документов ОУ;  - официальный сайт ОУ;  - официальная электронная почта ОУ;  - сеть Интернет посредством официального провайдера ОУ | - информация административно-хозяйственного содержания;  - финансовые документы;  - персональные данные сотрудников, воспитанников и их родителей (законных представителей) ОУ;  - организационно-правовая информация;  - материалы, регламентирующие организацию образовательного процесса в ОУ |
| 2 | Делопроизводи тель | - электронные базы официальных документов ОУ;  - официальный сайт ОУ;  - официальная электронная почта ОУ;  - сеть Интернет посредством официального провайдера ОУ | - информация административно-хозяйственного содержания;  - финансовые документы; персональные данные сотрудников и воспитанников ДОУ;  - организационно – правовая информация |
| 3 | Заведующая хозяйством | - электронные базы официальных документов ОУ; | - информация административно-хозяйственного содержания;  - финансовые документы;  - персональные данные сотрудников и воспитанников ОУ; |
| 4 | Педагогические работники | - электронные базы официальных документов ОУ; | - персональные данные сотрудников, воспитанников и их родителей (законных представителей) ОУ;  - организационно-правовая информация;  - материалы, регламентирующие организацию образовательного процесса в ОУ. |

**6. Права, ответственность должностных лиц,**

**ответственных за информационную безопасность обучающихся и сотрудников**

6.1. Должностные лица ответственных за информационную безопасность обучающихся и сотрудников вправе:

1). Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения, персональные данные сотрудников и обучающихся т.д.

2). Вносить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов, по организации и контролю доступа в сеть Интернет, к электронным базам официальных документов ОУ, на официальный сайт ОУ, в официальную электронную почту ОУ.

6.2. На должностных лиц, ответственных за информационную безопасность обучающихся и сотрудников, возлагается персональная ответственность в соответствии с действующим законодательством Российской Федерации за: качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением; разглашение информации административно-хозяйственного содержания и финансовых документов без согласования с заведующим ОУ среди лиц, не имеющих производственной принадлежности к МКУ «Управление образованием», Администрации Туринского городского округа, проверяющих и контролирующих органов; сохранность персональных данных обучающихся и сотрудников ОУ.

6.3. Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и развитию, влечет за собой ответственность в соответствии с действующим законодательством.

|  |  |  |
| --- | --- | --- |
|  |  | Приложение №1  к положению об обучении детей основам информационной безопасности на системном уровне, включая участие в занятиях по безопасности в информационной-телекоммуникационной системе «Интернет» и повышение медиаграмотности в МАДОУ детский сад №3 «Тополёк» |

**Детские безопасные сайты**

Каталог Вэб-браузеров для детей <http://browserss.ru/detskie-brauzery.php>

► [**Сайт «Единое окно доступа к образовательным ресурсам»**](http://window.edu.ru/catalog/) — информационная система «Единое окно доступа к образовательным ресурсам» предоставляет свободный доступ к каталогу образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования.

► [**http://www.saferunet.ru**](http://www.saferunet.ru/) — Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. А конкретнее – он занимаемся Интернет-угрозами и эффективным противодействием им в отношении пользователей.

► [**http://www.fid.su/projects/saferinternet/year/hotline**](http://detionline.com/) — Линия помощи «Дети онлайн». Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью.

► [**www.apkpro.ru**](http://www.apkpro.ru/) — электронный курс программы «Здоровье и безопасность детей в мире компьютерных технологий и Интернет». Программа представляет собой 72-х часовой курс, состоящий из 6 модулей. Каждый модуль программы дает подробное описание и рекомендации по обеспечению безопасной работы детей с компьютером и Интернетом.

► [**http://www.nedopusti.ru**](http://nedopusti.ru/) — социальный проект по защите прав детей «Не допусти» Организаторы проекта: Общественная палата РФ, РОЦИТ (Региональная Общественная Организация «Центр Интернет-технологий»), Межрегиональная правозащитная общественная организация «Сопротивление».

► [**http://www.newseducation.ru**](http://newseducation.ru/) — «Большая перемена» сайт для школьников и их родителей.

► [**http://www.smeshariki.ru/**](https://www.smeshariki.ru/?utm_expid=.40-lUqQQRTOJRvuYWcU2gA.0&utm_referrer=http%3A%2F%2Fds113.centerstart.ru%2Fnode%2F1338)- «Смешарики»: развлекательная соцсеть: игры, музыка, мультфильмы.

► [**http://www.solnet.ee/**](https://solnet.ee/)- «Солнышко»: детский портал.Развивающие, обучающие игры для самых маленьких и еще много интересного и для родителей.

► [**http://www.1001skazka.com**](http://www.1001skazka.com/) - «1001 сказка». На сайте можно скачать аудиофайлы — сказки, аудиокниги

|  |  |  |
| --- | --- | --- |
|  |  | Приложение №2  к положению об обучении детей основам информационной безопасности на системном уровне, включая участие в занятиях по безопасности в информационной-телекоммуникационной системе «Интернет» и повышение медиаграмотности в МАДОУ детский сад №3 «Тополёк» |

Должностная инструкция

ответственного за информационную безопасность и внедрение системы контентной фильтрации в МБДОУ д/с № 38 «Лесовичок»

1. Общие положения 1.1. Настоящий документ определяет основные обязанности, права и ответственность лица за информационную безопасность муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 38 «Лесовичок» (далее - Учреждение) 1.2. Ответственный за информационную безопасность назначается приказом руководителя Учреждения. 1.3. Ответственный за информационную безопасность осуществляет свою деятельность в интересах Учреждения в информационной сфере путем обеспечения защиты информации и поддержания достигнутого уровня защиты автоматизированных информационных систем (АИС) и ее ресурсов на всех этапах создания, модернизации и эксплуатации АИС. 1.4. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности Учреждения. Защита информации представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении технических и программных средств Учреждения и информации, циркулирующей в них. 1.5. Ответственный за информационную безопасность несет ответственность за реализацию принятой в Учреждение политики безопасности, закрепленной в Концепции информационной безопасности Учреждения. 1.6. Инструкция регулирует отношения между ответственным за информационную безопасность, пользователями АИС, сторонними организациями, возникающие при: - эксплуатации и развитии АИС; - формировании и использовании данных, сообщений, баз данных, информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления пользователю документированной информации; - при создании, внедрении и эксплуатации новых информационных технологий. 1.7. Ответственный за информационную безопасность обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты. 1.8. Требования ответственного за информационную безопасность, связанные с выполнением ими своих функций, обязательны для исполнения всеми пользователями АИС. 2. Обязанности ответственный за информационную безопасность Ответственный информационную безопасность обязан: 2.1. Обеспечить информационную безопасность, защиту конфиденциальной информации, в том числе и на бумажных носителях, от несанкционированного доступа, искажения и уничтожения при ее передаче, обработке и хранении с использованием средств вычислительной техники. 2.2. Организовывать доступ пользователей и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации. 2.3. Организовывать, в установленном порядке, передачу информации, составляющей коммерческую тайну Учреждения на сменных магнитных носителях и иными способами. 2.4. Организовывать сопровождение работ по категорированию объектов средств вычислительной техники Учреждения. 2.5. Знать перечень установленных в подразделениях Учреждения серверов, рабочих станций, средств копировально-множительной техники, устройств и топологию локально вычислительной сети. 2.6. Иметь перечень информационных ресурсов Учреждения. 2.7. Обеспечить доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения; 2.8. Осуществлять оперативный контроль за работой пользователей защищаемых рабочих станций, анализировать содержимое системных журналов всех PC и реагировать на возникающие нештатные ситуации. 2.9. Запрещать и немедленно блокировать применение пользователям сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС. 2.10. Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач. 2.11. Не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц. 2.12. Аппаратными и программными средствами выявлять факты несанкционированного доступа к информационным ресурсам АИС, а также другие нарушения, которые могут привести к разглашению или утрате конфиденциальной информации, и принимать меры по их пресечению. 2.13. Контролировать физическую сохранность средств и оборудования АИС. 2.14. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратнопрограммных средств защищенных рабочих станций и серверов. 2.15. Участвовать в приемке новых программных и аппаратных средств; 2.16. Периодически проверять состояние используемых СЗИ НС'Д. осуществлять проверку правильности их настройки. 2.18. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных рабочих станций 2.19. Вести контроль за процессом резервирования и дублирования важных ресурсов АИС. 2.20. Вести наблюдение за состоянием антивирусного контроля в организации. 2.21. Контролировать информацию, передаваемую по электронной почте, с целью исключения утечки конфиденциальной информации по открытым каналам связи в Учреждении. 2.22. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД. 2.23. Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требований по защите информации. 2.24. Вносить предложения для принятия решений о привлечении виновных к ответственности, за грубые нарушения требований нормативных документов по обеспечению сохранности конфиденциальной информации, а также о приостановке работ в случае обнаружения условий для утечки информации или материалов с пометкой для служебного пользования. 3. Права ответственного за информационную безопасность Ответственный за информационную безопасность имеет право: 3.1. Проводить мероприятия по защите конфиденциальной информации от несанкционированного доступа. 3.2. Требовать от сотрудников Учреждения соблюдения установленных технологий обработки информации и выполнения инструкций по защите информации. 3.3. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АИС. 3.4. Обращаться к руководителю Учреждения с требованием прекращения работы в АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями. 3.5. Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам ЛВС и БД или нарушивших другие требования по безопасности информации. 3.6. Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение. Ответственность лица, ответственного за информационную безопасность 4.1. Ответственный за информационную безопасность несет ответственность за качественное и своевременное выполнение задач, возложенных на него и изложенных в настоящей инструкции, а также определенных в текущих приказах и распоряжениях руководителя Детского сада 4.2. На ответственного за информационную безопасность возлагается персональная ответственность за программно-технические и криптографические средства защиты информации, и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

**Общие правила для родителей (законных представителей)**

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 в социальных сетях внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

 Проверьте, с какими другими сайтами связан сервер Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, 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 Интернете так же, как интересуетесь реальными друзьями.

**Возраст от 7 до 8 лет**

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

**Советы по безопасности в сети Интернет для детей 7-8 лет**

         Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.

         Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому, что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.

         Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

         Используйте специальные детские поисковые машины.

         Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

         Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

         Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

         Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

         Научите детей не загружать файлы, программы или музыку без вашего согласия.

         Не разрешайте детям использовать службы мгновенного обмена сообщениями.

         В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

         Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

         Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

         Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.