БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ОРЛОВСКОЙ ОБЛАСТИ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2020

УДК 004.056.5
ББК 74.202
М 54

Публикуется по решению редакционно-издательского совета
БУ ОО ДПО «Институт развития образования»

Рецензенты:

И. А. Патронова, к.п.н., директор БУ ОО ДПО «Институт развития образования».

А. А. Арабаджи, начальник отдела информационной безопасности администрации Губернатора и Правительства Орловской области.

Составитель: Тимофеева Л. Л., к. п. н., доцент кафедры развития образовательных систем БУ ОО ДПО «Институт развития образования»/

Методические рекомендации по обеспечению информационной безопасности в образовательной организации / сост. Л. Л. Тимофеева. — Орёл : Бюджетное учреждение Орловской области дополнительного профессионального образования «Институт развития образования», 2020. — 58. с.— Текст : непосредственный.

Методические рекомендации адресованы руководителям, педагогам и ответственным за обеспечение информационной безопасности образовательных организаций. Цель их разработки – разносторонняя поддержка направления работы образовательных организаций региона по обеспечению информационной безопасности. Пособие поможет специалистам актуализировать и дополнить свои представления о нормативно-правовых основах обеспечения информационной безопасности, о существующих рисках и угрозах в данной сфере; познакомиться с опытом региона и составить план работы по реализации основных направлений деятельности по обеспечению информационной безопасности в образовательной организации.

Оглавление

Актуальность проблемы обеспечения информационной безопасности в образовательной организации[1]

Термин «информационная безопасность» используется для обозначения двух различных понятий. В первом случае, ***информационная безопасность*** рассматривается как практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача обеспечения информационной безопасности в данном контексте — сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации[2]. Таким образом, речь идет о защите информации, о мерах, которые принимает образовательная организация по защите разных видов информации. *Актуальность* данного направления работы определяется увеличением числа угроз, связанных с цифровизацией и информатизацией системы образования, широким использованием дистанционных технологий, наличием противоречия между требуемой и имеющейся квалификацией специалистов, отвечающих за обеспечение информационной безопасности в образовательных организациях.

Также понятие «информационная безопасность» используется при обсуждении проблем безопасности обучающихся. В данном случае ***информационная безопасность*** рассматривается как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию»[3]. С позиций личностно ориентированного подхода информационная безопасность определяется как состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой. *Актуальность* задач образовательной организации, связанных с защитой детей от негативного влияния информации связана с возрастанием числа и спектра угроз, сопряженных с воздействием разных источников информации, формированием феномена «информационной социализации», наличием выраженного противоречия между требуемой и имеющейся квалификацией педагогов в рассматриваемой сфере.

Развитие человечества на современном этапе связано с постоянным возникновением новых вызовов, не наблюдавшихся ранее аспектов влияния на подрастающее поколение различных угроз. Так, с расширением спектра средств передачи информации и доступа к ним детей и подростков, увеличением доли различных форм дистанционного обучения на всех уровнях образования появ-

[1] Автор введения – Тимофеева Л.Л.

[2] NIST Interagency or Internal Report 7298: Glossary of Key Information Security Terms : [англ.] / Richard L. Kissel, editor, Computer Security Division, Information Technology Laboratory. — Revision 2. — Gaithersburg, MD, USA : National Institute of Standards and Technology, 2013. — 222 p.

[3] Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета – Федеральный выпуск № 5376 (297). 31.12.2010.

ляются новые риски социализации, угрозы для жизни и здоровья школьников, формируются инновационные направления деятельности взрослых по обеспечению информационной безопасности обучающихся. Увеличение доли различных форм дистанционного обучения на всех уровнях образования актуализирует проблему обеспечения безопасности обучающихся в информационно-телекоммуникационной сети Интернет.

Не менее важным является формирование у руководителей образовательных организаций и педагогов понимания необходимости отбора источников информации, ресурсов, печатной продукции, соответствующих требованиям информационной безопасности. Анализ проводимых в России исследований и практики работы образовательных организаций показывает низкий уровень осведомленности работников образования по данной проблеме, позволяет выделить направления работы по созданию безопасной информационной среды в образовательной организации.

Информационная среда является неотъемлемой частью образовательной среды современной образовательных организаций. *Образовательная среда* рассматривается как система условий организации жизнедеятельности, создаваемая сообразно с педагогическими целями и задачами[4]. *Информационную образовательную среду* в рамках проблемы информатизации образования определяют как «основанную на использовании компьютерной техники программно-телекоммуникационную среду, реализующую едиными технологическими средствами и взаимосвязанным содержательным наполнением качественное информационное обеспечение школьников, педагогов, родителей, администрацию учебного заведения и общественность»[5].

На основе Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» *информационная среда* как часть образовательной среды образовательной организации может быть определена как совокупность следующих компонентов: продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, зрелищные мероприятия. Таким образом, проблема обеспечения безопасности обучающихся в инфосфере не ограничивается вопросами защиты детей и подростков в информационно-телекоммуникационной сети Интернет. Необходимо в комплексе рассматривать все существующие угрозы:

- технологические угрозы, сопряженные с распространением вредоносных, шпионских программ, риском взлома защитных систем персонального компьютера;

- угрозы, связанные вредным или оскорбительным содержанием, с которым индивид сталкивается в сети Интернет;

- угрозы преследования обучающихся, включающие в себя любую форму нежелательных контактов, внимания, издевательства, насилия, связанные с коммуникацией в сети Интернет;

---

[4] Коджаспирова Г.М., Коджаспиров А.Ю. Педагогический словарь: Для студентов высш. и сред. пед. учеб. заведений. М.: Академия, 2001. – 176 с.

[5] Григорьев С.Г., Гриншкун В.В. Информатизация образования. Фундаментальные основы. Томск: ТМЛ-Пресс, 2008. – 286 с.

- угрозы, сопряженные с ситуацией раскрытия личной или конфиденциальной информации, персональных данных;

- угрозы, определяющие возникновение рисков социализации и негативных изменений в развитии личности детей и подростков, нанесение вреда их физическому и (или) психическому здоровью информацией, независимо от источника ее получения.

В соответствии с выделяемыми группами угроз определяются основные действия по обеспечению информационной безопасности детей в образовательной организации. Выделяют такой комплекс мер:

- правовая защита обучающихся, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в области обеспечения информационной безопасности;

- технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми;

- психолого-педагогические методы, направленные на работу с ребенком по формированию его медиа и компьютерной грамотности, стратегий поведения при встрече с нежелательным контентом и опасными знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др.[6]

В соответствии с принятыми научными подходами выделяют базовые направления обеспечения информационной безопасности обучающихся. Для уровня дошкольного образования это – меры по защите детей от негативного воздействия информации (по Н.А. Лызь – ограждающий подход), формирование предпосылок информационной культуры, культуры безопасности. Начиная с уровня начального общего образования все большее значение приобретают обучающий, образовательный и личностно-развивающий подходы (Н.А. Лызь), предполагающие формирование информационной культуры детей и подростков (Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих программы начального общего образования http://fgosreestr.ru/). В рамках ограждающего подхода необходимо выделить еще одно важное направление – использование методов анализа привлекаемых для осуществления образовательной деятельности ресурсов, всех компонентов информационной среды образовательной организации на предмет соответствия требованиям и критериям безопасности информации.

Анализ работы по созданию безопасной информационной среды в образовательных организациях Региональных инновационных площадок (РИП) «Создание современной образовательной среды для детей дошкольного возраста» и «Формирование культуры безопасности у детей младшего школьного возраста

[6] Шпагина Е.М., Чиркина Р.В. Компетентность педагогов и психологов в области информационной безопасности детей // Психология и право. 2019. Том 9. № 3. С. 261—277.

во внеурочной деятельности» позволяет построить пошаговый алгоритм действий:

- Изучение руководителями образовательной организации и педагогами научных и нормативно-правовых основ обеспечения информационной безопасности обучающихся. (Раздел 1).

- Разработка необходимых локальных актов по вопросам информационной безопасности в образовательной организации. (Приложение 1).

- Проведение самоаудита и последующее повышение компетентности участников образовательных отношений в решении задач обеспечения информационной безопасности детей и подростков. (Приложение 2).

- Оценка безопасности информационной среды образовательной организации. (Приложение 3).

- Проведение с родителями (законными представителями) воспитанников просветительской работы, нацеленной на повышение культуры информационной безопасности[7].

Таким образом, в сложившихся условиях одной из стратегических задач государственной политики в области информационной безопасности детей является обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России[8]. Среди актуальных задач образовательной системы региона сегодня выделяется «создание на территории Орловской области условий для обеспечения информационной безопасности детей, защиты от распространения информации, причиняющей вред их здоровью и (или) развитию».[9]

Целью разработки настоящих методических рекомендаций является разносторонняя поддержка направления работы образовательных организаций региона по обеспечению информационной безопасности. Методические рекомендации адресованы руководителям, педагогам и ответственным за обеспечение информационной безопасности образовательных организаций.

Составление методических рекомендаций направлено на решение следующих ***задач***:

- актуализация и дополнение представлений руководителей и педагогов о нормативно-правовых основах обеспечения информационной безопасности, о существующих рисках и угрозах в данной сфере;

- определение круга направлений деятельности по обеспечению информационной безопасности в образовательной организации;

- представление опыта региона по реализации основных направлений де-

[7] Письмо Минпросвещения России от 07.06.2019 N 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»).

[8] Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей».

[9] Из распоряжения губернатора Орловской области от 17 сентября 2018 года N 41-р «Об утверждении Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в Орловской области на 2018—2020 годы».

ятельности по обеспечению информационной безопасности в образовательной организации.

Методические рекомендации составлены по итогам реализации программ РИП «Формирование культуры безопасности у детей младшего школьного возраста во внеурочной деятельности» (Тимофеева Л.Л., Бутримова И.В.) и «Создание современной образовательной среды в ДОО» (проект «Информационная безопасность») (Тимофеева Л.Л., Бережнова О.В.), экспертной деятельности в сфере обеспечения информационной безопасности детей в сотрудничестве ООО «Национальная родительская ассоциация» (Тимофеева Л.Л., Королева Н.И.), социального партнерства с БОУ ТР ОО «ППМС-центр» (директор – Н.И. Королева), областным общественным экспертным Советом при Уполномоченном по правам ребенка в Орловской области (уполномоченный по правам ребенка – К.И. Домогатский), отделом информационной безопасности администрации Губернатора и Правительства Орловской области (начальник отдела – А.А. Арабаджи).

Результатом проделанной работы стали: разработка программы вебинара «Обеспечение информационной безопасности в образовательной организации: нормативно-правовые и методические аспекты», обобщение опыта инновационной и экспертной деятельности в форме выступлений на научно-практических конференциях, научных и методических публикаций (Приложение 4).

Конференции: III МНПК «Фундаментально-прикладные проблемы безопасности, живучести, надёжности, устойчивости и эффективности систем», посвященная 110-летию со дня рождения академика Н.А. Пилюгина (3—5.06.2019, г. Елец); Московский международный форум «Город Образования» (29.08.2019, г. Москва); Форум цифровой безопасности. Всероссийская Неделя безопасного Рунета (18.02.2020, г. Москва. Общественная палата РФ); IV ВНПК «Информационная безопасность и дети». Тема конференции: «Организация межведомственного сотрудничества в дополнительном образовании детей при формировании национальной политики информационной безопасности и медиаобразования» (27—28.02.2020, г. Москва); XI МК «Информационные технологии в управлении образованием. Дошкольное образование в цифровую эпоху» (14.05.2020, г. Москва); МНПК «Дистанционные образовательные технологии: опыт и перспективы» (28.05.2020, г. Орел); МНПК «Жизнь на дистанте: опыт пройденного и возможность повторения» (25.09.2020, г. Москва); Республиканская стратегическая конференция «Образование XXI века: инновации, преобразования, развитие» (23—26.09.2020, г. Сыктывкар); ВНПК «Цифровой ландшафт экосистемы дополнительного образования в контексте реализации национальных проектов» (11.12.2020, г. Москва); Региональный круглый стол «Безопасность ребенка в информационном обществе» (22.03. 2021, г. Орел); НПК «Актуальные вопросы обеспечения национальной безопасности России и здоровье нации» (20.05.2021, г. Москва, МПГУ); ВНПК «Актуальные вопросы безопасности в современном образовании» (27.05.2021, г. Екатеринбург); МНПК «Образовательное пространство в информационную эпоху» (8.06.2021, г. Москва, ФГБНУ «Институт стратегии развития образования РАО». Кафедра

ЮНЕСКО по глобальному образованию).

Проведены обучающие мероприятия, нацеленные на повышение компетентности участников образовательных отношений в решении задач обеспечения информационной безопасности: семинар «Обеспечение информационной безопасности детей дошкольного возраста» (5.02.2019 г. На базе МБДОУ д/с № 72), вебинар «Обеспечение информационной безопасности детей: специфика традиционного и дистанционного обучения» (21.09.2020 г. Совместно с издательством «Бином»); вебинар «Обеспечение информационной безопасности в образовательной организации: нормативно-правовые и методические аспекты» для дошкольных образовательных организаций. (18.05. 2021 г. Организаторы: Тимофеева Л.Л., доцент кафедры развития образовательных систем; Пухальская Н.М., методист отдела информатики и дистанционного обучения БУ ОО ДПО «Институт развития образования». Спикеры: Н.И. Королева. Л.Л. Тимофеева, А.А. Арабаджи. Модератор чата: Н.М. Пухальская. Материалы вебинара размещены на сайте ИРО: http://оиро.рф/wp-content/uploads/2021/05/Metodicheskie-materialy-vebinara_-Obespechenie-informacionnoj-bezopasnosti-v-BU-DOO_18.05.2021-g.zip).

Раздел 1. Нормативно-правовые основы обеспечения информационной безопасности в образовательной организации

Нормативные документы по обеспечению информационной безопасности обучающихся[10]

Федеральные законы РФ

Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».

Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Указы Президента РФ

Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

Постановления и распоряжения Правительства РФ

Концепция информационной безопасности детей. Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. No2471-р.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения общеобразовательных учреждениях».

Приказы Минкомсвязи России

Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей

[10] Обзор документов подготовила Н.И. Королева.
Ссылки на официальные сайты, где размещены перечисленные в разделе документы, представлены в перечне нормативных документов в разделе «Информационная безопасность» на сайте ИРО (http://xn--h1albh.xn--p1ai/informacionnaya-bezopasnost-2/).

вред их здоровью и (или) развитию».

Приказ Минкомсвязи России от 07.06.2019 № 261 «Об утверждении требований к подключению и доступу, включая требования к передаче данных, образовательных организаций, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных».

Региональные документы

Распоряжение губернатора Орловской области «Об утверждении Концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в Орловской области на 2018—2020 годы» от 17 сентября 2018 года N 41-р. http://docs.cntd.ru/document/550185239

План мероприятий по выполнению концепции по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей в орловской области на 2018—2020 годы. https://docs.cntd.ru/document/550185239/titles/JC76T9

Документы рекомендательного характера

Письмо департамента государственной политики в сфере оценки качества общего образования, Минпросвещения России № 04-474 от 07.06.2019 «О методических рекомендациях».

Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

Разработаны в рамках реализации пункта 7 приказа № 88 Минкомсвязи России 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы» Временной комиссией Совета Федерации по развитию информационного общества, Министерством просвещения России, Министерством цифрового развития, связи и массовых коммуникаций России и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Письмо Минкомсвязи России от 30.05.2019 №АВ-П17-062-11826 Методические рекомендации по основам информационной безопасности детей, находящихся в организациях отдыха детей и их оздоровления.

Письмо Департамента государственной политики в сфере общего образования Минпросвещения РФ № 03-39 от 29.03.2019 г. «О методических рекомендациях» Методические рекомендации по реализации мер, направленных на обеспечение безопасности и развития детей в сети «Интернет».

Письмо члена Совета Федерации Российской Федерации Боковой Л.Н.№66-02.41/ЛБ от 26.02.2019 г. Материалы в разделе «Проекты» сайта Единый урок. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

Нормативно-правовые основы обеспечения информационной безопасности в образовательной организации[11]

Защита информации (общие вопросы)

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденное Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 года № 912-51.
- «Перечень сведений конфиденциального характера», утвержден указом Президента Российской Федерации № 188 от 6 марта 1997 года.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России № 282 от 30 августа 2002 года.
- Постановление Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Персональные данные

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства Российской Федерации № 687 от 15 сентября 2008 года.
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальны-

[11] Обзор документов подготовил А.А. Арабаджи.
Ссылки на официальные сайты, где размещены перечисленные в разделе документы, представлены в перечне нормативных документов в разделе «Информационная безопасность» на сайте ИРО (http://xn--h1albh.xn--p1ai/informacionnaya-bezopasnost-2/).

ми органами».

- Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Критически важные объекты

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства Российской Федерации от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
- Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 года № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
- Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 года № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Государственные информационные системы

- Постановление Правительства Российской Федерации от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».
- Постановление Правительства Российской Федерации от 7 августа 2019 года № 1026 «О применении пункта 19.1 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».
- Приказ ФСТЭК России 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Нарушение правил защиты информации. КоАП РФ Статья 13.12.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение адми-

нистративного штрафа на граждан в размере от *одной тысячи пятисот* до *двух тысяч пятисот* рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от *двух тысяч пятисот* до *трех тысяч* рублей; на юридических лиц – от *двадцати тысяч* до *двадцати пяти тысяч рублей* с конфискацией несертифицированных средств защиты информации или без таковой.

Раздел 2. **Программные и аппаратные средства защиты информации**[12]

Разнообразие и количество средств защиты информации весьма велико. В наиболее общем виде их можно разделить на:

- физические средства защиты информации;
- аппаратные средства;
- программные (в том числе криптографические).

Подбор технических мер защиты для использования в конкретной организации опирается на концепцию информационной безопасности, принятую в регионе. Концепция обосновывает, что именно и каким образом необходимо защищать.

При построении системы защиты информации с использованием технических средств необходимо следовать определенным принципам:

- использование только лицензированного программного обеспечения (далее – ПО);
- использование только совместимого ПО, все части системы должны быть совместимыми друг с другом;
- управляемость, легкость администрирования системы, минимальное использование сторонней технической поддержки;
- протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, а также случаев несанкционированного доступа;
- затраты на организацию защиты информации должны быть соразмерны величине ущерба, который может быть нанесен собственнику информации.

Физические средства защиты информации

Физические средства защиты информации – это любые механические, электрические и электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним. К ним относятся:

- замки, в том числе электронные – один из простейших и эффективных способов физически ограничить доступ к чему-либо;
- экраны, жалюзи создают препятствия для визуального съема информации с систем обработки данных;
- системы контроля и управления доступом (СКУД) – задают правила доступа сотрудников к определенным помещениям;
- системы видеонаблюдения, видеорегистраторы – отслеживают перемещения работников, позволяют зафиксировать факт несанкционированного проникновения в защищаемые помещения;
- датчики, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения защищаемого оборудования – по сути «бюджетная версия» предыдущего пункта.

[12] Материал подготовил А.А. Арабаджи.

Аппаратные средства защиты информации

Аппаратные средства защиты информации – это любые устройства, которые либо затрудняют несанкционированный съем информации, либо помогают обнаружить потенциальные каналы утечки информации. Это самый узкоспециализированный класс средств защиты информации.

Насчитывается более десятка технических каналов утечки информации: акустические, виброакустические, оптико-электронные, паразитные электронно-магнитные импульсы и др. Соответственно, и борьба с утечкой ведется различными средствами: генераторы шума, сетевые фильтры, сканирующие радиоприемники и т.д.

Съем информации через технические каналы утечки возможен только при использовании специального, часто очень дорогостоящего оборудования. Как правило, информация, которой располагают образовательные организации, не является объектом попыток ее несанкционированного получения. В обычной деятельности организации из всех видов утечки информации по техническим каналам наиболее актуальными являются: просмотр информации с экранов дисплеев, бумажных и иных носителей информации (возможно, с помощью оптических средств) и прослушивание конфиденциальных переговоров, в том числе телефонных.

В данной ситуации могут использоваться как физические средства защиты информации, рассмотренные выше, так и организационные мероприятия. Также необходимо следовать правилам:

- не рекомендуется располагать защищаемые помещения на первых этажах зданий;
- независимо от этажа, следует закрывать окна жалюзи или экранами, в идеале для конфиденциальных мероприятий или обработки информации ограниченного распространения использовать помещения вообще без окон;
- использовать двойные двери с тамбурами;
- исключить пребывание посторонних в местах, где обрабатывается конфиденциальная информация;
- располагать мониторы таким образом, чтобы исключить просмотр информации с них посторонними;
- всегда блокировать рабочие станции при оставлении рабочего места. Для этого следует установить на компьютер пароль и при оставлении рабочего места производить выход из операционной системы. Необходимо также настроить компьютер на отключение при определенном периоде бездействия.

Программные средства защиты информации

Программные средства защиты информации – это программное обеспечение, предназначенные для решения задач, связанных с обеспечением информационной безопасности. Это самая многочисленная и распространенная группа средств защиты информации. К ним относят:

1. Средства операционных систем (далее – ОС). Современные ОС предоставляют широкий спектр встроенных решений по защите конфиденциальной информации на рабочих станциях и серверах:

- вход на свой компьютер, в рабочую группу, в домен происходит по паролю, смарт-карте, сертификату собственного удостоверяющего центра;

- минимизация прав при помощи учетных записей (локальных и доменных);

- ограничение прав с помощью локальной и групповой политик безопасности – запрет доступа к реестру, настройкам компьютера и др.;

- защита от угроз по сети при помощи встроенного брандмауэра;

- ограничение прав на доступ к общим ресурсам организации через механизм разрешений.

2. Антивирусные программы. Современные антивирусные средства кроме своих «основных обязанностей» умеют управлять доступом к съемным устройствам (запрет, белый список), сообщать об уязвимостях в установленном ПО, производить удаленную установку и удаление программ, шифровать данные на жестких дисках и съемных устройствах.

3. Программы резервного копирования и восстановления данных. Выделяют штатные программы резервного копирования, то есть встроенные в ОС и дополнительные, например, Acronis.

4. Прикладные программы, в которых существует разграничение прав пользователей – пароли, роли, и т.д.

5. Программные межсетевые экраны. Межсетевой экран – программа, контролирующая и фильтрующая на основе заданных правил входящий и исходящий сетевой трафик, определяет пропускать его или нет. Помимо этого, сетевой экран используется для защиты сети или рабочих станций от несанкционированного проникновения через уязвимости программного обеспечения или протоколов сети. Таким образом, межсетевой экран – это барьер между внутренней сетью организации, содержащей конфиденциальные или персональные данные, и глобальными информационными сетями. Если не хватает возможностей встроенного в Windows межсетевого экрана, используются программы и программно-аппаратные решения.

6. Прокси-серверы. Прокси-сервер – это компьютер, выполняющий роль посредника между пользователем и запрашиваемым адресом в сети интернет. Пользователь сначала подключается к прокси-серверу и запрашивает необходимый ресурс, расположенный на другом сервере. Например, почту или html-страницу. Затем прокси либо подключается к указанному серверу и получает у него ресурс, либо возвращает ресурс из собственного кэша.

Распространенные варианты использования прокси в компании:

- для повышения безопасности сети – шифрования запросов и скрытие адреса клиента, так как конечный сервер будет знать только адрес прокси;

- для увеличения производительности сети и экономии трафика за счет кэширования (запоминания на прокси) просмотренной информации и фильтрации трафика, например, блокировки рекламных блоков;

- для блокировки вредоносных и развлекательных сайтов и рекламы;

- для контроля использования сетевого канала;

- для мониторинга и регистрации веб-запросов пользователей.

Примерами могут служить такие прокси-серверы: платные – Kerio Control,

UserGate, WinGate, Traffic Inspector, бесплатные Squid и 3proxy.

7. Системы обнаружения и предотвращения вторжений. Считается, что в современных условиях защита, обеспечиваемая файерволом и антивирусом, уже недостаточно эффективна против сетевых атак злоумышленников. Причина в том, что вредоносное программное обеспечение может «замаскироваться» и отправлять сетевые пакеты, которые с точки зрения межсетевого экрана выглядят полностью легитимными. Антивирус плохо работает с еще неизвестными, неописанными угрозами. Повысить уровень защиты внутренней сети организации призваны системы обнаружения вторжений и системы предотвращения вторжений. Соответственно – IDS (Intrusion Detection Systems) и IPS (Intrusion Prevention Systems). Различия между ними заключаются лишь в том, что одна система может автоматически блокировать атаки, а другая просто предупреждает об этом сотрудника с помощью передачи сообщения на консоль управления, отправки электронного письма, SMS-сообщения на мобильный телефон и т.п.

В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS и IPS «заглядывают» внутрь передаваемого пакета, анализируя данные.

Приведем примеры систем IDS и IPS:

- СОВ Континент – это аппаратное решение IDS/IPS от компании «Код безопасности», которое имеет функцию контроля сетевых приложений.

- ViPNet IDS 3 (ИнфоТеКС) – программно-аппаратный комплекс для обнаружения вторжений на основе динамического анализа сетевого трафика стека протокола TCP/IP.

- Trend Micro TippingPoint — программно-аппаратное решение, выступающее в роли системы предотвращения вторжений нового поколения (NGIPS). Сочетает в себе новые технологии обеспечения сетевой безопасностью пользователей на уровне приложений, также TippingPoint проверяет входящий и исходящий трафик.

- InfoWatch ARMA Industrial Firewall – промышленный межсетевой экран нового поколения (NGFW). Позволяет своевременно обнаружить и заблокировать атаки на промышленные сети, защитить от несанкционированного доступа и обеспечить соответствие требованиям законодательства (№ 187-ФЗ и ФСТЭК России № 239, проходит сертификацию как МСЭ по типу «Д» и 4 классу защиты).

10. Системы контроля съемных носителей. Свыше 80% хищений информации сегодня происходит по вине собственных сотрудников, которые посредством использования различных типов USB-устройств скачивают конфиденциальную информацию. От этого не могут гарантировать технологии по защите сети от внешних злоумышленников. Для решения таких задач применяется установка контроля над использованием сменных носителей средствами операционной системы. Она стала возможна, начиная с Windows Server 2008 через использование групповых (локальных) политик.

Однако в настоящее время средства контроля внешних устройств – это одна из составных частей систем защиты от утечек конфиденциальной информа-

ции, или DLP-систем. Альтернативный подход к системе контроля съемных носителей – решение «Секрет Особого Назначения» от компании ОКБ САПР. Ключевая особенность продукта состоит в том, что легальность использования флешек определяется не ПК, к которым они подключаются, а самими USB-накопителями, то есть USB-накопитель работоспособен только на ограниченном количестве компьютеров, что делает бессмысленным его вынос с защищаемого объекта.

11. DLP и SIEM системы. На вершине программных средств защиты информации находятся DLP (Data Leak Prevention или Data Lost Protection или предотвращение утечек) и SIEM (Security Information and Event Management – управление информацией о безопасности и управление событиями безопасности) системы.

Основной задачей DLP-систем является предотвращение передачи конфиденциальной информации за пределы информационной системы. DLP-системы строятся на анализе информации, переходящей через периметр защищаемой информационной системы. При обнаружении в этой информации конфиденциальных сведений срабатывает активная компонента системы, и передача блокируется. Чтобы DLP-система срабатывала правильно, конфиденциальная информация должна быть предварительно отобрана (промаркирована).

SIEM-системы сами по себе не способны что-то предотвращать или защищать. Они предназначены для анализа информации, поступающей от различных других систем, таких как DLP, антивирусов, АРМ пользователей, серверов и выявления отклонения от норм по каким-то критериям. Выявляется отклонение – регистрируется инцидент информационной безопасности.

Кроме того, SIEM может предоставить всю необходимую доказательную базу, пригодную как для внутренних расследований, так и для суда. Это и есть одно из ее главных предназначений. При возникновении инцидента моментально оповещаются все заинтересованные лица.

Стоимость DLP- и SIEM-систем на 200 рабочих мест составит несколько миллионов рублей.

Среди таких систем:

Device Lock DLP от компании Смарт Лайн Инк;

Solar Dozor от Ростелекома, точнее от Ростелеком Солар;

InfoWatch Traffic Monitor от компании InfoWatch;

Symantec Data Loss Prevention от Symantec;

Контур безопасности от компании Search Inform.

Криптографические средства защиты информации

Криптографические средства защиты информации нужны для шифрования и кодирования информации с целью безопасной обработки, хранения и передачи ее по корпоративной или глобальной сети, для обмена шифрованными документами и организации безопасного удаленного взаимодействия, в том числе по сети Интернет.

Что нужно для организации такого взаимодействия? Если нужно только создавать и подписывать документы ЭП, хватит средств, перечисленных ниже в

пунктах 1-3. Для взаимодействия с удаленными филиалами и пользователями потребуются средства из пунктов 4-6.

1. Программные компоненты шифрования (криптопровайдеры). Криптопровайдер – это специальная программа-посредник, который позволяет операционной системе выполнять шифровальные функции, работающая по зарубежным или российским криптографическим стандартам. Наиболее популярны в России следующие криптопровайдеры:

КриптоПро CSP, разработка компании КриптоПро. Он работает под всеми популярными системами – Windows, Linux, Mac OS.

ViPNet CSP – бесплатный российский криптопровайдер от компании ИнфоТеКС, имеющий все необходимые сертификаты ФСБ.

Контнент АП производства российской компании «Код Безопасности»

2. Средства формирования и проверки ключей и электронной цифровой подписи предоставляют пользователю удобный графический интерфейс для зашифрования и расшифрования данных, создания и проверки электронной подписи (ЭП), для работы с сертификатами и криптопровайдерами:

КриптоАРМ от компании «Цифровые технологии»;

ViPNet PKI Client;

SignMachineW32 – бесплатное решение для электронной подписи, однако для его использования все-таки необходимо приобрести сертификат криптопровайдера КриптоПро CSP или VipNet CSP.

Для создания и проверки электронной подписи (ЭП) на веб-страницах, то есть в интернете, предназначен плагин (дополнение) для браузеров КриптоПро ЭЦП Browser plug-in.

Плагин легко встраивается и применим в любом из современных браузеров с поддержкой сценариев JavaScript.

3. Сами ключевые носители. Использование технологий ЭЦП для сотрудников подразумевает наличие надежного места для хранения закрытой части ЭЦП, а именно персональных носителей ключевой информации. Они в отличие от жесткого диска или флэшки пользователя обеспечивают защиту от несанкционированного считывания ЭЦП. Самые популярные из них – Рутокен (компания «Актив»), JaCarta от «Алладин РД» и Esmart USB от компании ISBC.

4. Средства для организации защищенных соединений и VPN. Если ранее речь шла о создании и обработке шифрованных документов, то крипто средства из этого и последующих разделов служат для обмена конфиденциальной информацией по публичным сетям передачи данных, в том числе сети Интернет.

Присоединить территориально удаленные филиалы и отдельных сотрудников, находящихся в командировке, к корпоративной сети компании призвана технология виртуальных частных сетей (VPN).

VPN – технология, которая позволяет подключаться к корпоративной сети компании через интернет, но по принципу доверенной частной сети по зашифрованному VPN каналу связи.

Комплексное решение в области VPN-технологий предлагает компания ИнфоТеКС. Ее ViPNet Client - это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-

клиента, персонального сетевого экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

5. Системы защищенной электронной почты. Системы защищенной электронной почты могут быть реализованы как:

- самостоятельные системы – Дипост, Диопост от компании Фактор-ТС;
- почтовый клиент Диопост предназначен для обмена зашифрованными и подписанными письмами по протоколам SMTP, POP3, TELNET.
- в составе пакета для организации защищенной сети, например, ViPNet «Деловая почта».

Программа ViPNet Деловая почта (или просто «Деловая почта») предназначена для организации электронного документооборота в защищенной сети ViPNet. С помощью «Деловой почты» пользователи сети ViPNet, у которых есть связь друг с другом, могут обмениваться электронными письмами.

6. Аппаратные криптомаршрутизаторы.

Криптографический шлюз (криптошлюз, криптомаршрутизатор, VPN-шлюз) – это программно-аппаратный комплекс для криптографической защиты трафика, передаваемого по открытым каналам связи, путем шифрования пакетов по различным протоколам.

Дионис NX от компании Фактор-ТС – это программно-аппаратный комплекс, имеющий в своем составе СКЗИ класса КС3, межсетевой экран 2-го класса защиты, систему обнаружения и предотвращения вторжений 2-го класса защиты.

Программно-аппаратные комплексы ЗАСТАВА — разработка российской компании ЭЛВИС-ПЛЮС. ПАК обеспечивает защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных защищенных сетей (VPN) на базе протоколов IPsec/IKE.

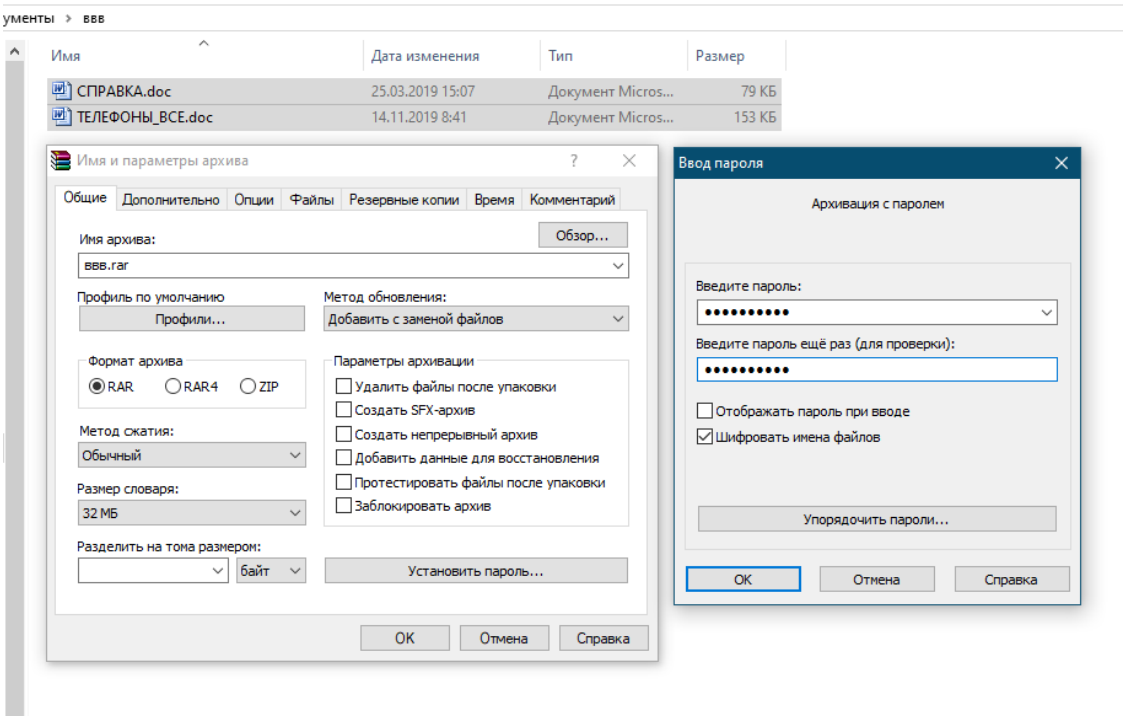
Аппаратно-программный комплекс шифрования «Континент» (АПКШ) — криптографический шлюз производства российской компании «Код Безопасности». АПКШ обеспечивает межсетевое экранирование и криптографическую защиту открытых каналов связи в соответствии с ГОСТ 28147.

Шифрование с помощью архиватора

Не стоит забывать, что шифровать файлы умеют также и популярные архиваторы WinRAR и 7-Zip. Так что обмениваться шифрованными файлами можно и без дополнительных средств криптографии. При этом нужно продумать способ безопасного обмена паролями шифрования.

Рассмотрим эту возможность на примере использования программы WinRAR.

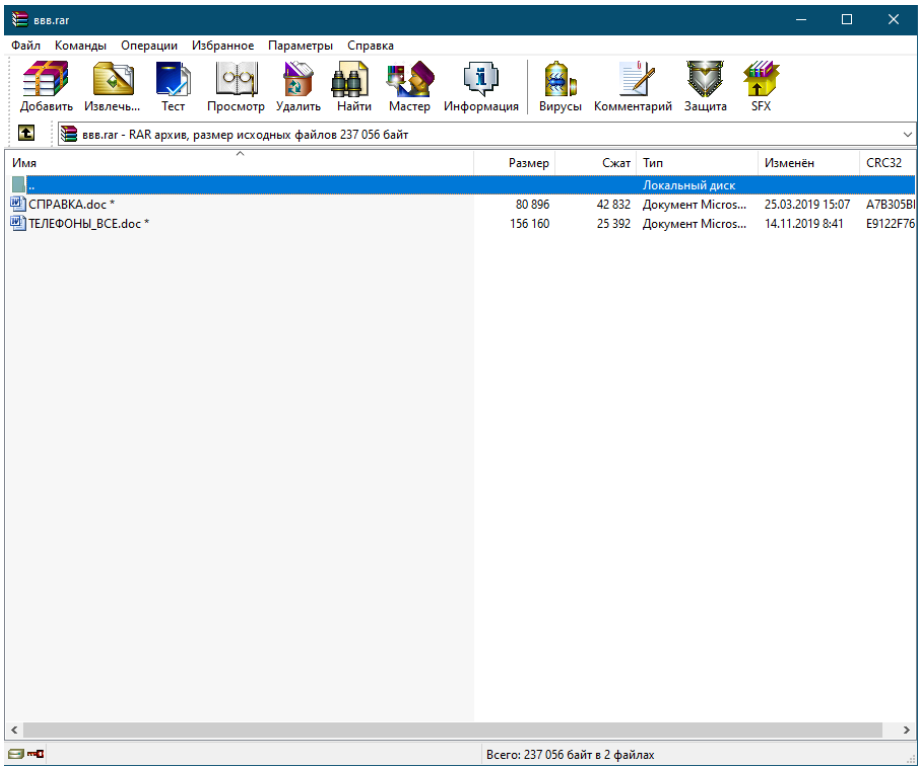
Выделяем в проводнике файлы, которые хотим защитить, и щелкаем правой кнопкой мышки. Выбираем в контекстном меню Добавить в архив…. В диалоге создания архива выбираем формат RAR, и нажимаем на кнопку Установить пароль…. Дважды вводим пароль (чем сложнее – тем лучше), и устанавливаем галочку Шифровать имена файлов. Жмем ОК:



После завершения, файлы будут защищены внутри архива. При попытке открыть архив пользователь получит запрос на ввод пароля.

Подобрать такой пароль считается невозможным, так как WinRAR использует AES-шифрование с длиной ключа 256 бит.

После ввода пароля можно увидеть содержимое архива.



Звездочки после имени файла указывают на то, что файлы зашифрованы, а красный ключ в левом нижнем углу говорит о том, что содержимое архива (имена файлов, комментарии и др.) также недоступно без ввода пароля.

Раздел 3. Деятельность образовательных организаций по обеспечению информационной безопасности обучающихся[13]

На основе результатов работы РИП «Создание современной образовательной среды для детей дошкольного возраста» и «Формирование культуры безопасности у детей младшего школьного возраста во внеурочной деятельности» разработан алгоритм действий руководителей и педагогов образовательных организаций по обеспечению информационной безопасности обучающихся:

- Изучение руководителями образовательной организации и педагогами научных и нормативно-правовых основ обеспечения информационной безопасности обучающихся. (Раздел 1).

- Разработка необходимых локальных актов по вопросам информационной безопасности в образовательной организации. (Приложение 1).

- Проведение самоаудита (Приложение 2) и последующее повышение компетентности участников образовательных отношений в решении задач обеспечения информационной безопасности детей и подростков.

- Оценка безопасности информационной среды образовательной организации. (Приложение 3).

- Проведение с родителями (законными представителями) воспитанников просветительской работы, нацеленной на повышение информационной культуры и культуры безопасности.

Профессиональная компетентность педагога в вопросах обеспечения информационной безопасности обучающихся

Большое значение имеет направление работы, связанное с повышением компетентности участников образовательных отношений в решении задач обеспечения информационной безопасности детей. Результаты опроса показывают, что далеко не все педагоги на должном уровне владеют знаниями и умениями, необходимыми для обеспечения информационной безопасности[14], соблюдения норм профессиональной этики[15], единые подходы к определению необходимых знаний и умений, трудовых действий специалистов[16] на основе профессионального стандарта Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании пока не разработаны. Опыт работы РИП позволяет выделить информационные блоки, с которыми необходимо ознакомить педагогов:

В документе «Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом

---

[13] Материал подготовили Тимофеева Л.Л, Бутримова И.В., Королева Н.И.

[14] Тимофеева Л.Л. Подготовка педагога к решению задач обеспечения безопасности детей дошкольного возраста // Вестник СурГПУ. 2020. № 1 (64). С. 119—128.

[15] Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности» (разработаны в соответствии с пунктом 8 приказа № 88 Минкомсвязи России от 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018—2020 годы»).

[16] Тимофеева Л.Л. Создание безопасной информационной среды в дошкольной образовательной организации // Детский сад от А до Я. 2020. № 1. С. 26—38.

информационных, потребительских, технических и коммуникативных аспектов информационной безопасности» (разработаны в соответствии с пунктом 8 приказа № 88 Минкомсвязи России от 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018—2020 годы») отмечается, что для эффективного решения проблем защиты детей от угроз, связанных с воздействием информации, необходимо обеспечить «охват не менее 70 процентов педагогических работников специальным обучением, направленным на повышение уровня их знаний и навыков в сфере информационной безопасности»[17].

На основе содержания профессионального стандарта «Педагог»[18] можно выделить основные задачи профессионального совершенствования (самосовершенствования) педагогов по трем направлениям: необходимые знания, трудовые действия, необходимые умения. Начальным этапом решения задач повышения компетентности педагогов по вопросам обеспечения информационной безопасности является проведение диагностических мероприятий (самоаудита – Приложение 3). Ниже мы представляем вариант содержания каждого из направлений на основе анализа различных документов и современных представлений о воздействии информации на развитие и здоровье детей[19] на примере педагогов дошкольного образования.

Необходимые знания. Педагог должен быть знаком с целями и задачами работы по защите детей от информации, причиняющей вред их здоровью и развитию, приоритетными направлениями, принципами и технологиями обеспечения информационной безопасности, представленными в нормативных документах федерального и регионального уровней. (Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ; Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ; Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ; Концепция информационной безопасности детей и др.).

Педагог должен владеть представлениями о роли информации в развитии детей, ее влиянии на процессы социализации в разные возрастные периоды, о подходах к формированию предпосылок становления информационной культуры в дошкольном возрасте, о компонентах информационной среды, типовых информационных угрозах, о критериях оценки и способах осуществления экспертизы информационной продукции для детей, о технических и программных средствах защиты детей от негативной информации, о современных тенденциях развития системы мер по обеспечению информационной безопасности до-

[17] https://www.xn--d1abkefqip0a2f.xn--p1ai/images/doc/metod/cyber.pdf

[18] Приказ Министерства труда и социальной защиты Российской Федерации от «18» октября 2013 г. № 544н об утверждении Профессионального стандарта Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) [Электронный ресурс]. URL: https://mosmetod.ru/metodicheskoe-prostranstvo/srednyaya-i-starshaya-shkola/geografiya/normativnye-dokumenty/professionalnyj-standart-pedagog-pedagogicheskaya-deyatelnost-v-sfere-doshkolnogo-nachalnogo-obshchego-osnovnog.html

[19] Тимофеева Л.Л. Повышение компетентности педагога по вопросам обеспечения информационной безопасности дошкольников // Детский сад от А до Я. 2020. № 2 (104) . С. 12—22.

школьников.

Среди ***трудовых действий*** на основе профессионального стандарта «Педагог» можно выделить: участие в создании безопасной и психологически комфортной информационной среды как составляющей образовательной среды детского сада; обеспечение информационной безопасности детей; планирование и реализация образовательной деятельности по формированию культуры безопасности, предпосылок информационной культуры в соответствии с федеральным государственным образовательным стандартом дошкольного образования; проведение оценки безопасности информационной среды дошкольной образовательной организации; участие в планировании и корректировке соответствующих организационных и образовательных задач в сотрудничестве с другими участниками образовательных отношений; развитие профессионально значимых компетенций, необходимых для обеспечения информационной безопасности детей.

Большое значение в профессиональной деятельности педагога имеет уровень сформированности ***необходимых умений***. Среди них можно выделить умения: анализировать объекты информационной среды образовательной организации, выявлять потенциальные угрозы; выбирать информацию, печатную и аудиовизуальную продукцию, соответствующую возрастным особенностям, интересам и потребностям детей; на элементарном уровне осуществлять экспертизу информационной продукции для детей; выбирать и применять наиболее эффективные методы формирования культуры безопасности, предпосылок становления информационной культуры в разные возрастные периоды в соответствии с индивидуальными особенностями детей; выстраивать партнерское взаимодействие с родителями (законными представителями) детей в вопросах обеспечения информационной безопасности воспитанников.

Остановимся подробнее на некоторых важных умениях.

Умение анализировать объекты информационной среды, на элементарном уровне *осуществлять экспертизу информационной продукции* для детей. По сути, обозначенный комплекс умений связан с четким знанием и способностью применять критерии оценки информационной продукции, выработанных на основе «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.

Рассмотрим примеры, поясняющие, как осуществляется анализ информационной продукции на основе отдельных критериев. Так информацией, побуждающей детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, можно признать, например, изображения, демонстрирующие опасные модели поведения как нормальные действия, то есть без иллюстрации их последствий и негативной оценки окружающими. Отрицательное воздействие такой информации может усиливаться инструктивным характером изображений (детали, пошаговые действия, показывающие, как реализовать то или иное действие); при выполнении опасных действий знакомым детям положительным (или любимым ими) персонажем, взрослым человеком, старшим ребенком; при выражении героем плаката положительных эмоций; при нереалистичном изображении происходящего.

Оправдывающими противоправное поведение могут быть признаны информационные продукты, демонстрирующие мнимую безобидность и безнаказанность соответствующих действий, их эмоциональную привлекательность. Эффект также, как и в первом примере, усиливается, если присутствует один или несколько рассмотренных выше вариантов подкрепления предлагаемой модели поведения. Обнаружение подобных характеристик свидетельствует о недопустимости использования в работе с детьми соответствующей информационной продукции.

Хотелось бы особо отметить некоторые моменты, которые нередко упускают из вида при анализе компонентов информационной среды даже опытные педагоги. Первый аспект: данные критерии относятся не только к приобретаемой образовательной организацией или родителями воспитанников информационной продукции. О них необходимо помнить и при совместной с детьми разработке различных средств наглядности (макетов, плакатов, моделей). Второй важный момент: анализируя информационную среду детского сада, педагоги чаще обращают внимание на используемые пособия, средства массовой информации, такие виды печатной продукции как афиши, плакаты, сценарии зре-

лищных мероприятий. При этом без внимания могут оставаться непосредственно проводимые ежедневно педагогические мероприятия, используемые детьми в быту и образовательной деятельности предметы. Необходимо обращать внимание на обложки тетрадей, блокнотов, альбомов, пеналы, оформление коробок карандашей, фломастеров и т.д.

Также крайне редко с позиций информационной угрозы анализируются материалы, используемые для обучения детей в области безопасности (плакаты, памятки, дидактические пособия, мультфильмы и т.д.). При этом данные материалы традиционно возглавляют топ-листы средств наглядности, нарушающих требования обеспечения информационной безопасности детей. На них можно увидеть пугающие изображения, разнообразные модели опасного поведения, негативные поведенческие установки. Так, ребенок дошкольного возраста, не понимая идеи плаката, может попытаться повторить увиденные действия, попасть в опасные ситуации. Некачественная информационная продукция приводит к усложнению развития ценностных ориентаций, личностно-смысловой сферы ребенка, усвоению дошкольниками просоциальных моделей поведения.

Подробнее вопросы о подходах и практических действиях по оценке безопасности информационной продукции представлены в серии статей, опубликованых в **журнале «Справочник старшего воспитателя»** (авт. Л.Л. Тимофеевой, Н.И. Королева):

№ 5-2021. Как оценить информационную безопасность мероприятий в детском саду. https://e.stvospitatel.ru/890451

№ 4-2021. Критерии и карты оценки, чтобы проверить информационную безопасность презентаций, видео и книг в детском саду.

https://e.stvospitatel.ru/880611

Как научить педагогов оценивать безопасность книг и мультфильмов для детей. Семинар-практикум. https://e.stvospitatel.ru/880613

№ 2-2021. Как оценить безопасность информационной среды детского сада. Критерии и карта экспресс-анализа. https://e.stvospitatel.ru/868683

Необходимость развития у воспитателей *умения формировать основы информационной культуры* оспаривается в связи с тем, что дошкольники не могут освоить знания, требуемые для обеспечения собственной информационной безопасности. Вместе с этим не подлежит сомнению тот факт, что дошкольное детство является важным этапом личностного развития, становления ценностно-смысловой сферы, формирования нравственных ориентиров, культуры безопасности, отношения к разного рода информации и способам ее получения. Таким образом могут быть выделены предпосылки формирования у детей способности обеспечивать собственную безопасность в информационной среде.

Важным условием для всех аспектов личностного становления является развитие субъектности [4]. В этом процессе педагог играет значительную роль, создавая ситуации «востребованности личности, ее сил саморазвития» (В.В. Сериков), выстраивая субъект-субъектные отношения с детьми. Сформированность субъектной позиции в период дошкольного детства позволяет индивиду в дальнейшем обрести психическую устойчивость, адаптивность, противостоять негативным воздействиям информации, не поддаваться манипулированию.

Умение выстраивать партнерское взаимодействие с семьями воспитанников в вопросах обеспечения информационной безопасности. Родители дошкольников часто недооценивают угрозы, связанные с информацией. Вследствие этого они некритически относятся к выбору мультфильмов, телепрограмм, игр, представляемых вниманию ребенка. В этом случае можно говорить о незрелости *мотивационного компонента родительской компетентности*, связанного со стремлением обеспечивать информационную безопасность ребенка сейчас и в дальнейшем, пониманием важности данного направления воспитания.

При построении взаимодействия с подобными семьями отправным пунктом должно стать ознакомление родителей воспитанников с угрозами, связанными с информацией, принципами построения системы работы по защите детей от ее негативного воздействия, ролью каждого из институтов социализации дошкольников в этой работе. Становление и развитие мотивационного компонента родительской компетентности – необходимое условие включения семьи во взаимодействие с образовательной организацией, в процессы обучения, самообразования, создания информационно безопасной среды в собственном доме.

Вместе с этим, сам факт мотивированности родителей к участию в реализации мер по защите ребенка от информационных угроз не определяет эффективность этой работы. Педагогу нужно уметь оказывать помощь семье в развитии знаниевого и деятельностного компонентов родительской компетентности. В этой работе можно выделить несколько направлений:

– просветительская деятельность – обучение и поддержка самообразования родителей, нацеленные на формирование у родителей необходимых представлений, умений и опыта;

– помощь в реализации мер по защите детей от информации, способной нанести вред их здоровью и (или) развитию, в условиях семьи с учетом полученных родителями (законными представителями) знаний, освоенных умений на основе согласования позиций семьи и образовательной организации;

– организация взаимодействия детей и родителей в процессе восприятия дошкольниками различной информации на основе освоенной взрослыми позиции посредника между ребенком и воспринимаемой им информацией, навыков оценки родителями действий, моделей поведения, передачи своего отношения к ним.

– обучение через семью – поддержка повседневной деятельности в рамках семейного воспитания, нацеленной на формирование предпосылок становления информационной культуры.

Развитие умения педагога выстраивать взаимодействие с семьями воспитанников по обеспечению информационной безопасности детей предполагает наличие представлений об отличительных особенностях семейного воспитания (специфика взаимоотношений родителей и ребенка, цели и методы воспитания), закономерностях обучения взрослых (учет стремления деятельно участвовать в обучении, привносить в обучающие ситуации собственный опыт и свои

жизненные ценности, соотносить содержание образовательного процесса со своими целями и задачами, проблемами в воспитании собственных детей, видеть возможности применения результатов для повышения качества жизни, нахождения ответов на волнующие обучающегося вопросы).

ПРИЛОЖЕНИЕ

Приложение 1

Обеспечение информационной безопасности образовательной организации. Необходимые дополнения и изменения, вносимые в локальные акты (на примере ДОО)[20]

(*фирменный бланк организации)*

УТВЕРЖДАЮ
Руководитель
_____
Приказ №_____
«__»_____20____г.

Примерное Положение об информационно-образовательной среде

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Федеральным Законом от 29 декабря 2012 г. № 273 – ФЗ «Об образовании в Российской Федерации»; Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных»

1.2. Информационно-образовательная среда (*далее – ИОС)* дошкольной образовательной организации *(далее – ДОО*) – открытая педагогическая система, направленная на формирование творческой, интеллектуальной и социально–развитой личности, сформированная на основе разнообразных информационных образовательных ресурсов, современных информационно–коммуникационных средств и педагогических технологий.[21]

1.3. ИОС ДОО включает в себя совокупность технологических средств (компьютеры, базы данных, коммуникационные каналы, программные продукты и др.), культурные и организационные формы информационного взаимодействия, компетентность участников образовательного процесса в решении учебно-познавательных и профессиональных задач с применением информационно-коммуникационных технологий (*далее - ИКТ*), а также наличие служб поддержки применения ИКТ.[22]

---

[20] Материалы подготовила Бережнова О.В., к. филол. н., доцент кафедры развития образовательных систем БУ ОО ДПО «Институт развития образования», на основе анализа опыта работы ДОО Региональной инновационной площадки «Создание современной образовательной среды для детей дошкольного возраста»

[21] *Дополнительная информация:*

- информатизация образования – один из приоритетов модернизации российского образования, главной задачей которой является создание единой информационно-образовательной среды (ИОС). ИОС рассматривается как одно из условий достижения нового качества образования;

- создание информационной образовательной среды направлено на улучшение организации управления и организации деятельности дошкольной образовательной организации и взаимодействия участников образовательного процесса.

[22] *Дополнительная информация:*

- информационная инфраструктура ИОС – программное обеспечение общего назначения (текстовые и графические редакторы, электронные таблицы и др.); программно-методическое обеспечение для организации обра-

1.5. Основные характеристики ИОС ДОО, значимые для организации образовательного процесса:

- *открытость,* которая обеспечивается за счет взаимодействия среды с информационно-образовательным пространством;
- *целостность,* за счет которой обеспечивается целесообразная логика развертывания образовательного процесса: постановка целей обучения, связанные с нею деятельность педагога, деятельность воспитанников и планируемый результат;[23]
- *полифункциональность* заключается в том, что среда может быть источником знаний и одновременно способствовать организации различных форм самостоятельной работы.

1.6. ИОС ДОО позволяет реализовать дидактические возможности инновационных технологий, эффективно организовать индивидуальную и коллективную работу воспитанников, обеспечивая тем самым целенаправленное развитие их самостоятельной познавательной деятельности.

2. Цели и задачи

2.1. Целями функционирования ИОС ДОО являются единство образовательного пространства ДОО, повышение качества образования, создание условий для поэтапного перехода к новому уровню образования на основе информационных технологий, создание условий для предоставления дистанционных образовательных услуг.

2.2. Основные задачи ИОС ДОО:

- возможность осуществлять в электронной (цифровой) форме планирование образовательного процесса;
- размещение и хранение материалов образовательного процесса, в том числе работ воспитанников и педагогов, используемых участниками образовательного процесса информационных ресурсов;
- фиксация хода образовательного процесса и результатов освоения основной образовательной программы дошкольного образования;
- взаимодействие между участниками образовательных отношений, в том числе дистанционное посредством сети Интернет, возможность использования данных, формируемых в ходе образовательного процесса для решения задач управления образовательной деятельностью;
- взаимодействие ДОО с органами, осуществляющими управление в сфере образования и с другими образовательными организациями;
- предоставление возможности быстрого доступа к данным по важнейшим показателям ДОО за любой период времени;
- реализация дифференцированного подхода к организации образовательного процесса;
- возможность повысить мотивацию воспитанников и их законных

зовательного процесса (обучающие и развивающие компьютерные программы, электронные справочники, мультимедийные энциклопедии и др.); информационные ресурсы ДООГ (единая база данных, мультимедийные образовательные разработки, хранилище документов, Web- сайт и др.).

[23] *Целостность возникает в результате сознательных действий субъектов образовательного процесса. Она конструируется с учетом вариативного выбора форм, методов и способов взаимодействия и способов получения образования.*

представителей;

- обеспечить наглядность представления практически любого материала;
- возможность обучать современным способам самостоятельного получения знаний

3. Структура ИОС ДОО

3.1 Структура ИОС ДОО включает следующие компоненты:

- *организационно-управленческий:* законодательные, нормативно-методические и распорядительные документы, должностные обязанности, инструкции и регламенты деятельности и управления ИОС;
- *программный:* операционные системы; прикладные программные средства; программно-методические комплексы, цифровые образовательные ресурсы;
- *методический*: учебно-методическая литература; демонстрационный материал; дидактический материал;
- *технический*: мультимедийный комплекс; принтеры, сканеры, компьютеры, планшеты, ноутбуки, интерактивные столы, интерактивные доски, информационные доски ДОО.[24]

4. Требования к ИОС ДОО

4.1. ИОС ДОО и отдельные ее компоненты создаются и используются в соответствии с действующим законодательством РФ в области образования, защиты авторских прав, защиты информации, а также реализуемыми в ДОО образовательными программами.

4.2 Обработка электронных ресурсов, содержащих персональные данные сотрудников и воспитанников, проводится строго в соответствии с нормами законодательства Российской Федерации на основании личного согласия сотруд-

---

[24] *Типовая организационная структура ИОС - центральный выделенный сервер для хранения единой базы данных ДОО и иных информационных ресурсов общего доступа;*
Техническая инфраструктура ИОС ДОО:

- *компьютерная техника (отдельные компьютеры, выделенный сервер);*
- *периферийное и проекционное оборудование (принтеры, сканеры, проекторы и др.);*
- *системное программное обеспечение.*

Информационная инфраструктура ИОС ДОО:

- *программное обеспечение общего назначения;*
- *программно-методическое обеспечение для организации образовательного процесса (обучающие и развивающие компьютерные программы, электронные справочники и др.);*
- *информационные ресурсы ДОО (единая база данных, учебно-методические банки данных, мультимедийные учебные разработки, хранилище документов, Web- сайт).*

Нормативно-организационное обеспечение ИОС ДОО:

- *ИКТ стратегия ДОО или программа информатизации ДОО, в которой описывается основные цели и задачи и этапы информатизации, приводится план мероприятий технической инфраструктуры на текущий учебный год (при достаточных материально финансовых ресурсах);*
- *распределение функций между сотрудниками ДОО, в том числе по управлению процессами информатизации, по техническому и методическому сопровождению, по обучению, консультированию, по внедрению информационных технологий в образовательную практику; регламентирующие документы, в том числе права и обязанности пользователей ИОС, все документы, регламентирующие защиту персональных данных, графики работы компьютерного оборудования и др.*

ников и родителей (законных представителей) воспитанников.[25]

4.3 Информационные ресурсы в ИОС не должны содержать информации, распространение которой нарушает законодательство Российской Федерации.

5. Права и обязанности пользователей ИОС ДОО

5.1. Пользователями ИОС ДОО являются администрация ДОО, сотрудники ДОО, воспитанники ДОО, родители воспитанников (законные представители)

5.2. Права пользователей ИОС ДОО разграничиваются в соответствии с должностными обязанностями и содержанием информационных запросов и потребностей.

5.3. Администрация ДОО обязана:

- организовывать взаимодействие всех участников образовательного процесса в рамках ИОС;
- разрабатывать и организовывать принятие всех локальных актов ДОО, регламентирующих сферу ИОС;
- осуществлять контроль над деятельностью пользователей ИОС ДОО;
- использовать автоматизированные информационные системы в управлении образовательном процессе ДОО;
- организовывать восстановление работоспособности программных, технических и методических компонентов после разных аварийных ситуаций в короткие сроки;
- постоянно повышать свою ИКТ – компетентность;
- организовывать непрерывное повышение ИКТ – компетентности всех сотрудников ДОУ;
- обеспечивать информационную безопасность;
- заранее предоставлять необходимые материалы для размещения информации на сайте и информационных стендах ДОО.

5.4. Администрация ДОО имеет право:

- на общение в информационном пространстве с участниками образовательного процесса;
- на размещение, обновление и удаление информации о деятельности ДОО;
- на ввод, хранение, обработку персональных данных сотрудников и воспитанников в пределах объема должностных обязанностей;
- на осуществление телекоммуникационного обмена в сети Интернет с использованием официальных адресов ДОО;
- на разработку организационно-управленческих технологий реализации ИОС ДОО;

5.5. Сотрудники ДОО обязаны:

- использовать возможности новых информационных технологий в об-

---

[25] *К информационным ресурсам структурных подразделений, служб и объектов инфраструктуры относятся: лицензионные операционные системы, прикладные программные средства, программные компоненты информационных сред; файлы баз данных.*
Несанкционированное использование и копирование информационных ресурсов структурных подразделений, служб и объектов инфраструктуры не допускается.

разовательной деятельности;

- создавать и размещать в информационном пространстве ДОО электронные методические пособия, презентации, материалы конкурсов, выставок, педагогические проекты;
- повышать свою квалификацию в области ИКТ;
- создавать личные сайты с методическими консультациями и рекомендациями для родителей (законных представителей) детей и педагогического сообщества;
- бережно относиться к компьютерной технике ДОО, сообщать о замеченных поломках.

5.6. Сотрудники ДОО имеют право:

- готовить методические материалы (материалы для выступлений, материалы для конкурсов, педагогические проекты, презентации, аналитические отчеты, индивидуальные консультации и рекомендации для родителей (законных представителей) детей и педагогического сообщества), размещать их на сайте ДОО и в методическом кабинете.
- пользоваться необходимой информацией, находящейся в методическом кабинете, а также в сети Интернет, использовать электронную почту, и электронные образовательные ресурсы;
- подбирать методическое обеспечение для НОД;
- использовать в НОД и режимных моментах ДОО мобильную мультимедийную технику;
- использовать сайт ДОО и образовательные порталы в своей работе;
- на научно-методическую и консультационную поддержку в освоении новейших информационных технологий;
- создавать видеотеку группы (фото и видеосъемку НОД и режимных моментов с детьми) и пользоваться фондом медиатеки и видеотеки ДОО;
- размещать свою информацию на сайте и информационных стендах ДОО.

5.7. Родители (законные представители) воспитанников имеют право:

- ознакомиться на сайте ДОО с уставными документами, публичным отчетом;
- узнавать информацию о мероприятиях ДОО, знакомиться с фото и видеоархивами.

5.8. Воспитанники имеет право:

- участвовать в индивидуальной и коллективной работе группы с использованием элементов ИОС ДОО

5.9. Воспитанники обязаны:

- соблюдать правила пользования ИОС ДОО.

6. Ограничения и запреты на деятельность пользователей ИОС

6.1. Пользователи ИОС ДОО обязаны предпринимать только разрешенные в явной форме действия с данными,

6.2. Пользователям ИОС ДОО запрещается:

- намеренно негативно влиять на работу информационных систем;
- менять чужие данные, кроме специальных, явно оговоренных случаев;

- не допускать рассылки информации, существенная часть адресатов которой не предполагала получить ее или могла бы возражать против получения;
- принимать меры по ответственному хранению средств ИКТ, полученных для индивидуального или группового использования, не оставлять их без присмотра, не допускать порчи оборудования;
- принимать разумные меры по предотвращению запрещаемых выше действий другими участниками образовательных отношений;
- получение информации из Интернета или с цифровых носителей должно соответствовать целям и задачам образовательного процесса, в частности, запрещается просмотр сайтов, не предназначенных для знакомства с ними детьми до 18 лет.

7. Ответственность пользователей ИОС ДОО

7.1 Ответственность пользователей ИОС ДОО за совершение противоправных деяний наступает в соответствии с административным и уголовным кодексом РФ[26]

7.2 Основаниями для привлечения пользователей ИОС – сотрудников ДОО к материальной ответственности является причинение вреда программным или техническим компонентам ИОС ДОО.

8. Срок действия Положения

8.1 Положение действует до принятия нового.

Дополнения в должностные инструкции педагога ДОО

2.1. Общие положения

Должен знать:

- законодательство Российской Федерации в сфере обеспечения информационной безопасности детей;

- основные методы и способы защиты детей от информации, не совместимой с задачами образования и воспитания, иной противоправной информации, информации, причиняющей вред здоровью и развитию детей.

2.2. Должностные обязанности

- планирует использование сети Интернет в образовательном процессе с учетом специфики программы;

- незамедлительно принимает меры, направленные на прекращение доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение

---

[26] *Возмещение вреда, причиненного имущественным и смежным правам, совершенное с использованием компонентов ИОС наступает в соответствии с гражданским кодексом РФ.*

Дисциплинарная и материальная ответственность пользователей ИОС – сотрудников ДОО, наступает в соответствии с трудовым кодексом, Законом Российской Федерации «Об образовании», коллективным договором, правилами внутреннего трудового распорядка, Уставом образовательного учреждения и настоящим Положением.

Основаниями для привлечения пользователей ИОС – сотрудников ДОО к дисциплинарной ответственности являются нарушения эксплуатации компонентов ИОС, правил внутреннего трудового распорядка, должностных обязанностей и настоящего Положения.

которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в порядке, установленном правилами использования сети Интернет в ДОО

- при случайном обнаружении ресурса, содержание которого не имеет отношения к образовательной деятельности, пользователь обязан незамедлительно ограничить доступ к информационным ресурсам и сообщить об этом ответственному лицу за организацию доступа к сети Интернет в ДОО.

2.4. Ответственность

Несет ответственность за:

- невыполнение требований законодательства Российской Федерации в сфере обеспечения информационной безопасности детей;

- несоблюдение порядка использования сети Интернет в ДОО

При использовании сети Интернет в ДОО пользователи несут персональную ответственность в соответствии действующим законодательством Российской Федерации, а также:

- за содержание передаваемой, принимаемой и печатаемой информации.

- за нанесение любого ущерб оборудования в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния и т.п.).

(фирменный бланк организации)

СОГЛАСОВАНО Председатель первичной профсоюзной организации _____ «__»_____20____г.	УТВЕРЖДАЮ Руководитель _____ Приказ №_____ «__»_____20____г.

Примерная Инструкция
по организации контроля использования сети Интернет

1. Общие положения

1.1. Использование сети Интернет в дошкольной образовательной организации (*далее – ДОО*) направлено на решение административных задач и задач образовательного процесса.

1.2. Настоящая Инструкция регламентирует порядок осуществления контроля использования сети Интернет в ДОО.

1.3. Пользователями сети Интернет в ДОО являются администрация ДОО, сотрудники ДОО, воспитанники ДОО.

2. Контроль использования сети Интернет

2.1. Контроль использования сети Интернет направлен на предотвращение использования сети Интернет в целях, не совместимых с задачами образовательного процесса, иных целях, запрещенных в соответствии с Правилами использования сети Интернет ДОО.

2.2. Контроль использования сети Интернет в ДОО осуществляется лицом, ответственным за обеспечение доступа к ресурсам сети Интернет. Использование сети Интернет сотрудниками ДОО допускается в целях исполнения ими своих должностных обязанностей. Использование сети Интернет сотрудниками ДОО в личных целях не допускается.

2.3. Использование воспитанниками сети Интернет допускается только при условии осуществления контроля сотрудником ДОО. Во время доступа воспитанников ДОО к сети Интернет в рамках занятий учебного плана контроль использования сети Интернет осуществляет сотрудник ДОО, ответственный за организацию доступа к сети Интернет, а именно:

- наблюдает за использованием технических средств и сети Интернет воспитанниками;

- принимает меры по пресечению поиска и получения информации, не совместимой с задачами образовательного процесса, обращений к ресурсам сети Интернет, не имеющим отношения к образовательному процессу;

- незамедлительно принимает меры, направленные на прекращение и ограничение доступа воспитанников к информации, не совместимой с задачами образовательного процесса, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей, а также информирует об инциденте руководителя ДОО.

Доступ воспитанников к сети Интернет вне занятий не осуществляется.

2.4. Контроль использования сети Интернет работниками ДОО осуществляется через:

- проведение периодического контроля состояния системы обеспечения информационной безопасности;
- проверку соблюдения работниками ДОО обязанностей, предусмотренных должностной инструкцией;
- текущий контроль эксплуатации технических средств контентной фильтрации;
- контроль организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в образовательной организации;
- контроль функционирования технических средств, применяемых при организации доступа к сети Интернет, и их конфигурации (компьютерное оборудование, системное и прикладное программное обеспечение);
- контроль изменения конфигурации технических средств, применяемых при организации доступа к сети Интернет.

2.5. В случае обнаружения попыток поиска и получения информации, не совместимой с административными задачами и задачами образования и воспитания, обращений к ресурсам сети Интернет, не имеющим отношения к образовательному процессу, лицо, ответственное за обеспечение доступа к ресурсам сети Интернет, немедленно сообщает об инциденте руководителю ДОО с целью проведения профилактической работы, направленной на предотвращение использования сети Интернет в непредусмотренных целях.

2.6. Контроль использования сети Интернет сотрудниками ДОО может

осуществляться в виде проводимого с установленной периодичностью анализа электронного журнала регистрации/истории/ посещения ресурсов Интернет. При этом в электронном журнале регистрации посещений ресурсов сети Интернет должна быть отражена следующая информация: фамилия, имя, отчество сотрудника ДОО или уникальный идентификатор, время посещения ресурса сети Интернет, адрес ресурса сети Интернет.

В случае отсутствия в ДОО технической возможности ведения электронного Журнала Журнал ведется в печатном варианте и содержит следующую информацию: фамилия, имя, отчество сотрудника ДОО, допущенного к использованию сети Интернет, время посещения ресурса сети Интернет, адрес ресурса сети Интернет, личная подпись лица. Страницы данного Журнала должны быть пронумерованы, прошиты и скреплены печатью ДОО.

(фирменный бланк организации)

СОГЛАСОВАНО Председатель первичной профсоюзной организации _____ «__»_____20____г.	УТВЕРЖДАЮ Руководитель _____ Приказ №_____ «__»_____20____г.

Примерная должностная инструкция
ответственного за организацию доступа к сети интернет

1. Общие положения

1.1 Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам назначается на должность и освобождается от должности руководителем ДОО.

1.2 Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам руководствуется в своей деятельности Конституцией и законами РФ, государственными нормативными актами органов управления образования всех уровней, Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; локальными актами ДОО, а также настоящей должностной инструкцией.

1.3 Ответственный за работу в сети Интернет и ограничение доступа к информационными нтернет-ресурсам подчиняется непосредственно руководителю ДОО.

2. Права и обязанности ответственного за организацию доступа к сети Интернет

2.1 Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам должен знать:

- законодательство Российской Федерации в сфере обеспечения информационной безопасности детей;

- основные методы и способы защиты детей от информации, не совместимой с задачами образования и воспитания, иной противоправной информации, информации, причиняющей вред здоровью и развитию детей.

2.2 Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам выполняет следующие виды работ:

- планирует использование сети Интернет в ДОО;
- обеспечивает доступ к сети Интернет в ДОО;
- обеспечивает установку и настройку технических средств контентной фильтрации;
- разрабатывает политики доступа к ресурсам сети Интернет, применяемые в технических средствах контентной фильтрации;
- разрабатывает организационно-распорядительные документы ДОО по вопросам использования сети Интернет;
- организует и осуществляет контроль использования сети Интернет в ДОО;
- осуществляет периодический контроль системы обеспечения информационной безопасности обучающихся, систематически проводит контроль функционирования технических средств контентной фильтрации;
- обеспечивает информирование работников ДОУ о порядке использования сети Интернет;
- следит за состоянием компьютерной техники и Интернет-канала «точки доступа к Интернету»;
- в случае необходимости инициирует обращение к поставщику Интернет-услуг (оператору связи); осуществляет контроль ремонтных работ;
- в случае необходимости лимитирует время работы пользователя в Интернете;
- в случае получения сведений об интернет-ресурсе, содержание которого не имеет отношения к образовательному процессу, ответственный направляет информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток). Передаваемая информация должна содержать доменный адрес ресурса, сообщение о тематике ресурса, дату и время обнаружения, информацию об установленных в ДОО технических средствах ограничения доступа к информации;
- участвует в организации повышения квалификации сотрудников по использованию Интернета в профессиональной деятельности;
- осуществляет регулярное обновление антивирусного программного обеспечения;
- контролирует проверку пользователями внешних электронных носителей информации (CD-ROM, флеш-накопителей) на отсутствие вирусов;
- следит за приходящей корреспонденцией на адрес электронной почты ДОО;
- планирует использование ресурсов сети Интернет в образовательной организации на основании заявок работников образовательной организации;
- разрабатывает, представляет на педагогическом совете образователь-

ной организации проект Правил организации доступа к сети Интернет в образовательной организации;

- организует получение сотрудниками образовательной организации электронных адресов и паролей для работы в сети Интернет и информационной среде образовательной организации;
- организует контроль использования сети Интернет в образовательной организации;
- организует контроль работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;
- систематически повышает свою профессиональную квалификацию, включая ИКТ- компетентность, компетентность в использовании возможностей Интернета в образовательном процессе;
- проводит инструктаж сотрудников по правилам работы с используемыми средствами и системами защиты информации;
- принимает участие в создании и обновлении официального сайта ДОО;
- выполняет регулярно резервное копирование данных на сервере, при необходимости восстанавливают потерянные или поврежденные данные.[27]

2.3. Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам вправе:

- Определять политику доступа к ресурсам сети Интернет, применяемые в технических средствах контентной фильтрации.
- Участвовать в административных совещаниях при обсуждении вопросов, связанных с использованием Интернета в образовательном процессе и управлении ДОО.
- Отдавать распоряжения пользователям «точки доступа к сети Интернет» в рамках своей компетенции.
- Ставить вопрос перед руководителем ДОО о нарушении пользователями «точки доступа к сети Интернет» правил техники безопасности, противопожарной безопасности, поведения, регламента работы в Интернете.
- Определять ресурсы сети Интернет, используемые в учебном процессе на основе запросов педагогов.

3. Ответственность ответственного за организацию доступа к сети Интернет

3.1 Ответственный за организацию доступа к сети Интернет несет ответственность за:

- невыполнение требований законодательства Российской Федерации в сфере обеспечения информационной безопасности детей;
- несоблюдение порядка использования сети Интернет в ДОО;

[27] *Возможные варианты дополнений:*
- Принимает участие в создании (и актуализации) веб-ресурсов ДОО.
- Обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения.
- Соблюдает правила использования сети Интернет.
- Отслеживает работу антивирусных программ, проводят один раз в неделю полную проверку компьютеров на наличие вирусов.

- ненадлежащее и своевременное выполнение обязанностей, возложенных на него настоящей должностной инструкцией;
- несоблюдение Правил техники безопасности, противопожарной безопасности и норм охраны труда в ДОО;
- состояние делопроизводства по вверенному ему направлению работы;
- невыполнение правил использования ресурсов сети Интернет и ограничения доступа, установленного в образовательной организации, а также за работоспособность систем контентной фильтрации.

(*фирменный бланк организации)*

УТВЕРЖДАЮ
Руководитель
_____
Приказ №_____
«__»_____20____г.

Примерное Положение
о защите детей от информации, причиняющей вред их здоровью и (или) развитию

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 29 декабря 2010г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» с изменениями от 28.07.2012 №139-ФЗ, от 05.04.2013 №50-ФЗ, от 29.06.2013 №135-ФЗ, от 02.07.2013 №185-ФЗ, от 14.10.2014 №307-ФЗ, от 29.06.2015 №179-ФЗ, от 01.05.2017 №87-ФЗ, от29.07.2018 №242-ФЗ, от 18.12.2018 №472–ФЗ; приказом Министерства связи и массовых коммуникаций РФ от 16 июня 2014г. № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», для обеспечения административных и организационных мер по защите от информации, причиняющей вред их здоровью и развитию.

1.2. К информации, причиняющей вред их здоровью и (или) развитию детей, относится информация:

- запрещенная для распространения среди детей;
- распространение которой среди детей определенных возрастных категорий ограничено.

1.2.1. К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, 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, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

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.

3. К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

2. Классификация информационной продукции

2.1. Осуществление классификации информационной продукции.

2.1.1. Классификация информационной продукции осуществляется ее производителями и (или) распространителями самостоятельно.

2.1.2. Классификация информационной продукции осуществляется по следующим категориям информационной продукции:

1) информационная продукция для детей, не достигших возраста шести лет;

2) информационная продукция для детей, достигших возраста шести лет;

3) информационная продукция для детей, достигших возраста двенадцати лет;

4) информационная продукция для детей, достигших возраста шестнадцати лет;

5) информационная продукция, запрещенная для детей.

2.1.3. Классификация информационной продукции, предназначенной и (или) используемой для обучения и воспитания детей в организациях, осуществляющих образовательную деятельность по реализации основных общеобразовательных программ, осуществляется в соответствии с федеральным законодательством.

2.1.4. Сведения, полученные в результате классификации информационной продукции, указываются ее производителем или распространителем в сопроводительных документах на информационную продукцию и являются основанием для размещения на ней знака информационной продукции и для ее оборота на территории Российской Федерации.

2.2. Информационная продукция для детей, не достигших возраста шести лет

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 ее 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).

2.3. Информационная продукция для детей, достигших возраста шести лет.

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 ее жанром и (или) сюжетом:

1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;

2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти 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.

3. Условия присутствия воспитанников при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для воспитанников, в случае их организации и (или) проведения

3.1. Вся информация, используемая во время проведения публичных мероприятий в ДОО, подлежит классификации. При проведении публичного мероприятия, публичного исполнения может использоваться информационная продукция для детей, не достигших возраста шести лет – «0+», информационная продукция для детей, достигших возраста шести лет – «6+»:

- презентационные и видеоматериалы, являющиеся иллюстрацией к проводимому мероприятию,
- учебные пособия, рекомендуемые или допускаемые к использованию в образовательном процессе в соответствии с законодательством Российской Федерации в области образования;
- телепрограммы, телепередачи, транслируемые в эфире без предварительной записи;
- информационная продукция, распространяемая посредством радиовещания и на официальном сайте ДОО;
- информационная продукция, демонстрируемая посредством зрелищных мероприятий.
- элементы, используемые при оформлении сцен, спектаклей, книжных выставок и др.

3.2. Оборот информационной продукции, содержащей информацию, предусмотренную статьей 5 Федерального закона «О защите детей от информации причиняющей вред их здоровью и развитию», без знака информационной продукции не допускается.

3.3. Воспитанники могут присутствовать на публичном показе, при публичном исполнении, зрелищном мероприятии, если на них не демонстрируется информационная продукция:

- побуждающая воспитанников к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у воспитанников 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;
- 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;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

3.4. Ответственность за использование информационной продукции во время публичного мероприятия в ДОО несет лицо, ответственное за проведение мероприятия, назначенное приказом руководителя.

При организации присутствия воспитанников на публичном показе в ДОО, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции:

- до начала демонстрации посредством зрелищного мероприятия информационной продукции проверяется знак информационной продукции. В случае демонстрации нескольких видов информационной продукции для воспитанников разных возрастных категорий в зрелищном мероприятии может использоваться только информация, разрешенная для младшей возрастной категории;
- указанный знак размещается на афишах и иных объявлениях о проведении зрелищного мероприятия, а также на входных билетах, приглашениях и иных документах, предоставляющих право его посещения. Знак информационной продукции размещается в публикуемых программах теле- и радиопередач, перечнях и каталогах информационной продукции, а равно и в такой информационной продукции, размещаемой в информационно-телекоммуникационных сетях;
- лица, организующие и проводящие показы, демонстрации и другие мероприятия публичного характера несут ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию в соответствии с законодательством Российской Федерации.[28]

---

[28] *Дополнительные требования к обороту информационной продукции, запрещенной для детей и ее фрагментов, распространяемых посредством эфирного и кабельного, теле – и радиовещания, сети Интернет и сетей подвижной радиотелефонной связи, в местах доступных для детей.*

1. Информационная продукция, причиняющая вред здоровью и (или) развитию детей, не подлежит распространению посредством теле- и радиовещания.

2. Распространение посредством телевизионного вещания информационной продукции, содержащей информацию, запрещенную для детей, сопровождается демонстрацией знака информационной продукции в углу кадра, в начале трансляции телепрограммы, телепередачи, а также при каждом возобновлении их трансляции (после прерывания рекламой и (или) иной информацией).

3. Распространение посредством радиовещания информационной продукции, содержащей информацию, запрещенную для детей, за исключением радиопередач, транслируемых в эфире без предварительной записи, сопровождается сообщением об ограничении распространения такой информационной продукции среди детей в начале трансляции радиопередач.

4. При размещении анонсов или сообщений о распространении посредством теле- и радиовещания информационной продукции, запрещенной для детей, не допускается использование фрагментов указанной информационной продукции, содержащей информацию, причиняющую вред здоровью и (или) развитию детей.

4.5. Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», в местах, доступных для детей, предоставляется лицом, ответственным за доступ к сети «Интернет» в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

4. Процедуры присвоения и размещения знака информационной продукции и (или) текстового предупреждения об информационной продукции, запрещенной для детей

4.1. Обозначение категории информационной продукции знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения информационной продукции среди детей осуществляется с соблюдением требований настоящего Федерального закона ее производителем и (или) распространителем следующим образом:

1) применительно к категории информационной продукции для детей, не достигших возраста шести лет, - в виде цифры «0» и знака «плюс»;

2) применительно к категории информационной продукции для детей, достигших возраста шести лет, - в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шести лет»;

4.2. Производитель, распространитель информационной продукции размещают знак информационной продукции и (или) текстовое предупреждение об ограничении ее распространения среди детей перед началом демонстрации фильма при кино- и видеообслуживании в порядке, установленном уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти. Размер знака информационной продукции должен составлять не менее чем пять процентов площади экрана.

4.3. Размер знака информационной продукции должен составлять не менее чем пять процентов площади афиши или иного объявления о проведении соответствующего зрелищного мероприятия, объявления о кино- или видеопоказе, а также входного билета, приглашения либо иного документа, предоставляющих право посещения такого мероприятия.

4.4. Знак информационной продукции размещается в публикуемых программах теле- и радиопередач, перечнях и каталогах информационной продукции, а равно и в такой информационной продукции, размещаемой в информационно-телекоммуникационных сетях.

4.5. Текстовое предупреждение об ограничении распространения информационной продукции среди детей выполняется на русском языке, а в случаях, установленных Федеральным законом от 1 июня 2005 года N 53-ФЗ «О государственном языке Российской Федерации», на государственных языках республик, находящихся в составе Российской Федерации, других языках народов Российской Федерации или иностранных языках.

5. Меры защиты детей от информации, причиняющей вред их здоровью и (или) развитию

5.1. Список лиц ответственных за меры защиты детей от информации, причиняющей вред их здоровью и (или) развитию, устанавливается приказом по ДОО.

5.2. Ознакомление работников, в трудовые обязанности которых входит

---

6. Информационная продукция, запрещенная для детей, не допускается к распространению в предназначенных для детей образовательной организации, или на расстоянии менее чем сто метров от границ территорий указанных организаций.

организация и осуществление оборота информационной продукции, запрещенной для детей, с положениями законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию и настоящим Положением.

5.3. Контроль за соответствием содержания и художественного оформления печатных изданий, полиграфической продукции (в т.ч. тетради, дневники, обложки для книг, закладки для книг) иной информационной продукции, используемой в образовательном процессе, требованиям, предъявляемым к информационной продукции для детей соответствующей возрастной группы, осуществляется работниками ДОО в соответствии их должностными обязанностями и родителями обучающихся в соответствии с их обязанностями, а также с учетом обозначения категории информационной продукции.

6. Процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию

6.1. Назначение сотрудника, ответственного за применение административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещенной для детей, и за проверку порядка их применения.

6.2. Ознакомление работников ДОО с Правилами работы в сети Интернет и настоящим Положением.

6.3. Осуществление контроля за использованием ресурсов сети Интернет в образовательном процессе.

6.4. Ведение журналов учета работы с ресурсами сети Интернет в точках доступа сети Интернет.

6.5. Установка специальных технических средств контентной фильтрации.

6.6. Отправка оператору организации, осуществляющей по договору контентную фильтрацию, сведений о выявленных ресурсах, содержащих информацию, запрещенную законодательством РФ и не совместимую с задачами образования и воспитания, для ограничения доступа к этим ресурсам.

6.7. Рассмотрение в срок, не превышающий десяти рабочих дней со дня получения, обращений, жалоб или претензий о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

6.8. Установление в течение десяти рабочих дней со дня получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, причин и условий возникновения такого доступа и принятие мер по их устранению.

7. Ответственность за правонарушения в сфере защиты детей от информации причиняющей вред их здоровью и развитию

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

Приложение 2.

Примеры вопросов анкеты для осуществления самоаудита «Обеспечение информационной безопасности детей дошкольного возраста в ДОО»[29]

НЕОБХОДИМЫЕ ЗНАНИЯ

1. Считаете ли Вы, что в современном мире значительно возросло влияние средств массовой информации, массовых коммуникаций на процессы социализации детей?

А. Да

Б. Нет

2. Как Вы, думаете, может ли информация оказывать негативное влияние на детей дошкольного возраста?

А. Да

Б. Нет

3. Выберите одно или несколько определений понятия «информационная безопасность детей».

А. Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Б. Состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В. Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Г. Защита ребенка от дестабилизирующего воздействия информационной продукции и создание информационной среды, способствующей позитивной социализации и индивидуализации, развитию детей, сохранению их здоровья и благополучия.

4. Согласны ли Вы с утверждением, что в последние годы значительно расширился спектр угроз, исходящих от различных видов информационной продукции?

А. Да

Б. Нет

5. Считаете ли Вы необходимым обеспечение информационной безопасности детей дошкольного возраста?

А. Да.

Б. Нет.

Обоснуйте свой ответ

6. Кто, по Вашему мнению, в первую очередь несет ответственность за обеспечение информационной безопасности ребенка?

А. Семья (близкие взрослые)

Б. Образовательные организации

В. Организации, создающие информационную продукцию

[29] Анкета разработана Л.Л. Тимофеевой, Н.И. Королевой, Т.А. Родиной.

Г. Государственные структуры, контролирующие информационную безопасность детей

Ваш вариант

7. Назовите основные федеральные документы, регулирующие действия образовательной организации по обеспечению информационной безопасности детей.

8. Как вы считаете, могут ли представлять угрозу для детей компоненты информационной среды детского сада?

А. Да

Б. Нет

9. Если Вы ответили «Да» на предыдущий вопрос, отметьте виды информационной продукции, которые могут представлять опасность для здоровья и (или) развития детей?

А. Средства массовой информации.

Б. Печатная продукция (книги, буклеты, плакаты, дидактические материалы, изображения на обложках тетрадей, альбомов и т.д.).

В. Аудиовизуальная продукция на любых видах носителей.

Г. Игры, игрушки.

Д. Зрелищные мероприятия.

Е. Информация, распространяемая посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет».

10. Знакомы ли Вы с критериями классификации информационной продукции для детей?

А. Да

Б. Нет

11. Известно ли Вам, какое влияние может оказывать информация на различные сферы личности ребенка?

А. Да

Б. Нет

12. Приведите примеры негативного влияния на отдельные сферы личности.

А. Мотивационная

Б. Ценностно-смысловая

В. Эмоциональная

Г. Познавательная

ТРУДОВЫЕ ДЕЙСТВИЯ

1. Принимаете ли Вы участие в создании безопасной и психологически комфортной информационной среды детского сада?

А. Да

Б. Нет

2. В зависимости от ответа на вопрос № 1 приведите примеры своего участия в создании безопасной информационной среды или поясните, почему не участвуете в данной работе.

3. Принимаете ли Вы участие в работе по обеспечению информационной безопасности детей?

А. Да

Б. Нет

Поясните свой ответ по аналогии с работой над вопросом № 2.

4. Осуществляете ли Вы планирование и реализацию образовательной деятельности по формированию культуры безопасности, предпосылок информационной культуры?

А. Да

Б. Нет

Поясните свой ответ по аналогии с работой над вопросом № 2.

5. Являетесь ли Вы участником работы экспертной группы по оценке безопасности информационной среды дошкольной образовательной организации (ДОО)?

А. Да

Б. Нет

Поясните свой ответ по аналогии с работой над вопросом № 2.

5. Осуществляете ли Вы развитие профессионально значимых компетенций, необходимых для обеспечения информационной безопасности детей?

А. Да

Б. Нет

Поясните свой ответ по аналогии с работой над вопросом № 2.

НЕОБХОДИМЫЕ УМЕНИЯ

Оцените по 10-балльной шкале свои профессиональные умения

Умение	Самооценка
Анализировать объекты информационной среды образовательной организации, выявлять потенциальные угрозы	
Выбирать информацию, печатную и аудиовизуальную продукцию, соответствующую возрастным особенностям, интересам и потребностям детей	
Осуществлять экспертизу информационной продукции для детей	
Выбирать и применять эффективные методы формирования культуры безопасности, предпосылок становления информационной культуры	
Выстраивать партнерское взаимодействие с родителями детей в вопросах обеспечения информационной безопасности воспитанников	

Приложение 3.

Примеры карт оценки безопасности информационной продукции

Бланк экспресс-анализа информационной продукции[30]

Название информационной продукции _____

Параметры оценки	**Отметка / Баллы**
1. Разновидность информационной продукции[31]	
продукция средств массовой информации	
печатная продукция	
аудиовизуальная продукция на любых видах носителей	
зрелищные мероприятия	
2. Категория информационной продукции	
информационная продукция для детей, не достигших возраста шести лет («0+»)	
информационная продукция для детей, достигших возраста шести лет («6+»)	
3. Соблюдение требований к информационной продукции, установленных законодательством о защите детей от информации, причиняющей вред их здоровью и развитию	
наличие возрастной маркировки («0+» или «6+»)	
соответствует заявленной возрастной категории	
не побуждает детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, либо жизни и (или) здоровью иных лиц	
не способна вызвать у детей желание употребить запрещенные вещества, табачные изделия, осуществлять противоправные действия	
не обосновывает и не оправдывает допустимость насилия и (или) жестокости, не побуждает осуществлять насильственные действия по отношению к людям или животным[32]	
не отрицает семейные ценности, не пропагандирует нетрадиционные сексуальные отношения, не формирует неуважение к родителям и (или) другим членам семьи	
не представлена в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия	
не представлена в виде изображения или описания нена-	

[30] Составители: Тимофеева Л.Л., Королева Н.И. Бланк составлен на основе Федерального закона от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»: статьи 2, 5, 7, 8, 12.

[31] В пунктах 1—3 отмечается соответствие (несоответствие) информационной продукции описанию.

[32] За исключением случаев, предусмотренных ФЗ 436.

сильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий	
не содержит ненормативную лексику, бранные слова и выражения, не относящиеся к нецензурной брани	
не вызывает у детей страх, ужас или панику	
не содержит материалы, противоречащие требованиям российского законодательства, нарушающие нормы нравственности и морали	
не содержит персональные данные, распространяемые с нарушением закона	
4. Образовательный потенциал информационной продукции[33]	
имеет познавательную, воспитательную направленность	
соответствует потребностям и интересам детей	
способствует развитию гармоничной личности, позитивного мышления, воображения	
текст соответствует правилам и нормам родного языка	
оформление соответствует требованиям к качеству и размеру элементов изображения, цветам, их сочетанию, не вызывает негативных эмоций и психологических реакций	

Оценка результатов анализа

В работе с детьми может использоваться информационная продукция, получившая отметки по всем позициям в пункте 3, набравшая не менее 10 баллов в пункте 4.

Чек-лист «Анализ печатной и аудиовизуальной продукции»[34]

Виды информационной продукции	**Критерии оценки**					
	1	**2**	**3**	**4**	**5**	**6**
Печатная продукция						
периодические детские издания						
художественная литература						
познавательная литература						
учебные пособия (тетради на печатной основе, раскраски)						
наглядно-дидактические пособия						
тематические плакаты						

[33] В пункте 4 информационная продукция оценивается в баллах от 1 до 3.

[34] Составители: Королева Н.И., Тимофеева Л.Л.

лэпбуки						
демонстрационный и раздаточный материал						
настольно-печатные игры, пазлы						
оформление материалов для детского творчества (обложки альбомов, тетрадей, блокнотов, бумаги для аппликации, коробки с красками, пластилином)						
наклейки						
портфолио детей						
рекламные объявления, афиши						
Аудиовизуальная продукция						
видео- и аудиоматериалы, слайд-фильмы						
мультфильмы						
художественные фильмы						
обучающие, развивающие фильмы						
видеоролики, видеосюжеты						
телепередачи						
диафильмы						
аудиокниги, аудиоспектакли						
компьютерные игры						
мобильные планетарии						
музыкальные мягкие игрушки						
аудиозаписи песен						
рингтоны телефонов						
компьютерные презентации						

Приложение 4.

Публикации по теме «Информационная безопасность образовательной организации»

1. Тимофеева Л.Л. Обеспечение информационной безопасности детей дошкольного возраста // Дошкольное воспитание. 2019. № 7. С. 4—10.
2. Тимофеева Л.Л. Компетентность педагога в обеспечении информационной безопасности детей дошкольного возраста // Образование в Орловской области. 2019. № 1. С. 43—53.
3. Тимофеева Л.Л. Создание безопасной информационной среды в дошкольной образовательной организации // Детский сад от А до Я. 2020. № 1. С. 26—38.
4. Тимофеева Л.Л., Королева Н.И. Характеристика компетентности педагога по вопросам обеспечения информационной безопасности на основе профессионального стандарта «Педагог» // Внешкольник. 2020. № 1 (193). С. 11—12.
5. Тимофеева Л.Л. Подготовка педагога к решению задач обеспечения безопасности детей дошкольного возраста // Вестник СурГПУ. 2020. № 1 (64). С. 119—128.
6. Тимофеева Л.Л. Повышение компетентности педагога по вопросам обеспечения информационной безопасности дошкольников // Детский сад от А до Я. 2020. № 2 (104) . С. 12—22.
7. Тимофеева Л.Л. Повышение компетентности педагогов в вопросах информационной безопасности младших школьников // Дистанционные образовательные технологии: опыт и перспективы. Сборник научных статей Международной научно-практической онлайн конференции. 28 мая 2020 года, г. Орел. Бюджетное учреждение Орловской области дополнительного профессионального образования «Институт развития образования», 2020. – 344 с. – ISBN 978-5-9909476-1-0. С. 78—83.
8. Тимофеева Л.Л. Педагогические аспекты проблемы обеспечения информационной безопасности детей дошкольного и младшего школьного возраста // Цифровизация как драйвер роста науки и образования: [монография / Аюпова Г. Т. и др.]; под общей ред. М. В. Посновой. Петрозаводск : МЦНП «Новая наука», 2020. – 263 с. С. 99—112.
9. Тимофеева Л.Л. Организация работы образовательных организаций по обеспечению информационной безопасности детей // Лидер образования. Выпуск 12.2020. С. 10—41.
10. Тимофеева Л.Л. Как оценить безопасность информационной среды детского сада. Критерии и карта экспресс-анализа // Справочник старшего воспитателя дошкольного учреждения. 2021. № 2. С. 4–8.
11. Тимофеева Л.Л., Королева Н.И. Критерии и карты оценки, чтобы проверить информационную безопасность презентаций, видео и книг в детском саду // Справочник старшего воспитателя дошкольного учреждения. 2021. № 4. С. 29–36.

12. Тимофеева Л.Л., Королева Н.И. Как научить педагогов оценивать безопасность книг и мультфильмов для детей. Семинар-практикум // Справочник старшего воспитателя дошкольного учреждения. 2021. № 4. С. 44–50.

13. Тимофеева Л.Л. Злодеи и хулиганы на утреннике, или Как оценить информационную безопасность мероприятий в детском саду // Справочник старшего воспитателя дошкольного учреждения. 2021. № 5.

14. Тимофеева Л.Л. От чего надо защищать детей: три шага, чтобы рассказать родителям про информационную безопасность// Справочник старшего воспитателя дошкольного учреждения. 2021. № 6. С. 46—51.

Приложение 5.

Сведения об авторах разделов методических рекомендаций

Арабаджи А.А., начальник отдела информационной безопасности администрации Губернатора и Правительства Орловской области.

Бережнова О.В., к. филол. н., доцент – руководитель кафедры развития образовательных систем БУ ОО ДПО «Институт развития образования», федеральный эксперт программ дополнительного профессионального образования, эксперт Комитета по профессиональным квалификациям в области школьного образования Совета по профессиональным квалификациям в сфере образования, федеральный эксперт, член Президиума федерального экспертного совета Всероссийской общественной организации «Воспитатели России», член редакционного совета и авторского коллектива комплексной образовательной программы дошкольного образования «Мир открытий».

Бутримова И.В., к. филол. н., старший методист отдела начального общего образования, БУ ОО ДПО «Институт развития образования», федеральный эксперт программ дополнительного профессионального образования, эксперт в сфере федерального государственного контроля (надзора) в сфере образования.

Королева Н.И., директор БОУ ТР ОО «ППМС-центр», аккредитованный эксперт Роскомнадзора, эксперт НРА, член областного общественного экспертного Совета при Уполномоченном по правам ребенка в Орловской области, член экспертного Совета Межрегиональной общественной организации «Национальный совет социальной информации».

Тимофеева Л.Л., к.п.н., доцент кафедры развития образовательных систем БУ ОО ДПО «Институт развития образования», Федеральный эксперт ООО «Национальная родительская ассоциация», эксперт президиума Федерального экспертного совета по дошкольному образованию «Воспитатели России». Автор парциальной программы «Формирование культуры безопасности у детей 3—8 лет», соавтор пособий предметной линии «Окружающий мир» (ГК «Просвещение»), член редакционного совета и авторского коллектива комплексной образовательной программы дошкольного образования «Мир открытий», член редколлегии журналов «Воспитатель ДОУ», «ОБЖ. Основы безопасности жизнедеятельности», член редсовета журнала «Лидер образования».