Министерство общего и профессионального образования Свердловской области
Государственное автономное образовательное учреждение
дополнительного профессионального образования Свердловской области
«Институт развития образования»

Технологии обеспечения информационной безопасности в образовательном учреждении (организации)

методические рекомендации
для руководителей и педагогов образовательных учреждений
(организаций)

Екатеринбург
2014

ББК 32.973.26-018.2я81
Т58

Т 58 Технологии обеспечения информационной безопасности в образовательном учреждении (организации) : метод. рекомендации для руководителей и педагогов образовательных учреждений (организаций) / авт.-сост. Н. Ю. Сероштанова, Е. В. Тюгаева, Н. В. Шпарута ; Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». – Екатеринбург : ГАОУ ДПО СО «ИРО», 2014. – 44 с.

Методические рекомендации по технологиям обеспечения информационной безопасности в образовательном учреждении (организации) предназначены для руководителей и педагогов, заинтересованных в создании и успешном функционировании системы информационной безопасности учреждения (организации), обеспечивающей защиту и хранение персональных данных участников образовательного процесса, защиту информации компьютеров и мобильных устройств локальной сети образовательной организации от вирусного программного обеспечения, ограничение доступа обучающихся к нежелательной информации в Интернете.

Материалы помогут руководителям образовательных учреждений (организаций) оценить уже существующую систему информационной безопасности, определить направления усовершенствования системы для ее эффективного функционирования.

Рекомендации предназначены для использования в системе повышения квалификации руководителей и педагогов образовательных учреждений как очно, так и дистанционно.

ББК 32.973.26-018.2я81

Содержание

Введение

Обеспечение информационной безопасности образовательной организации является одним из основных направлений информатизации и, в целом, функционирования образовательной организации (далее ОО). Информационная безопасность является условием и одним из критериев эффективности деятельности ОО.

В федеральных нормативных документах устойчивого словосочетания «информационная безопасность» не используется, употребляются такие понятия, как «защита информации», «доступ к информации», «конфиденциальность персональных данных» и другие. В данных методических рекомендациях под *«информационной безопасностью образовательной организации»* мы понимаем *состояние защищенности персональных данных субъектов образовательного процесса, обучающихся от информации, причиняющей вред их здоровью и развитию, информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.*

Система информационной безопасности образовательной организации включает в себя следующие компоненты:

1. Правовой – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
2. Организационный – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
3. Программно-технический – это использование различных алгоритмических, программных и аппаратных средств, препятствующих нанесению ущерба.

Необходимо уточнить, что необходимым условием для функционирования системы безопасности ОО является проведение мероприятий для педагогов, обучающихся и родителей, с целью развития компетенций, связанных с работой на компьютерных устройствах, поиском и обработкой информации в Интернете, защитой от «вредной» информации.

В системе информационной безопасности образовательной организации можно выделить следующие направления:

- организация контентной фильтрации данных из Интернета на компьютерных устройствах, используемых учениками;
- обеспечение антивирусной защиты и других интернет-угроз компьютеров и мобильных устройств локальной сети организации;
- обеспечение защиты персональных данных субъектов образовательного процесса;

— организация правомерного использования объектов авторского права.

В данных методических рекомендациях рассматриваются механизмы для реализации вышеперечисленных направлений в образовательных организациях общего и среднего профессионального образования. Кафедра информационных технологий ГАОУ ДПО СО «ИРО» реализует дополнительные профессиональные программы и семинары повышения квалификации в области информационной безопасности для руководителей и педагогов образовательных организаций, в рамках которых у слушателей:

1. Формируются и развиваются профессиональные компетенции в области информационной безопасности, по следующим направлениям:
— разработка системы информационной безопасности ОО;
— подготовка пакета внутренних нормативных документов и инструкций для функционирования системы информационной безопасности;
— выбор и организация работы контентной фильтрации, антивирусных программ на компьютерных устройствах сети ОО;
— разработка системы защиты персональных данных субъектов образовательного процесса;
— разработка системы защиты информационных ресурсов ОО;
— проведение мероприятий с участием субъектов образовательного процесса для повышения уровня информационной культуры в области информационной безопасности.
2. Усовершенствуются следующие трудовые действия:
— участие в разработке и реализации программы развития образовательной организации в целях создания безопасной и комфортной образовательной среды;
— регулирование поведения обучающихся для обеспечения безопасной образовательной среды.
— развитие у обучающихся познавательной активности, самостоятельности, инициативы, творческих способностей, формирование гражданской позиции, способности к труду и жизни в условиях современного мира, формирование у обучающихся культуры здорового и безопасного образа жизни.
3. Развиваются следующие необходимые умения:
— общепедагогическая и предметно-педагогическая ИКТ-компетентности;
— выявление совместно с обучающимися недостоверных и малоправдоподобных данных.

Данные методические рекомендации позволят оптимизировать процесс обучения на программах повышения квалификации, где рассматриваются вопросы информационной безопасности образовательной организации, а также окажут методическую помощь педагогам-практикам в создании, усовершенствовании системы информационной безопасности образовательной организации в соответствии с существующими нормативно-правовыми документами.

Нормативные документы по информационной безопасности в образовательной организации

Основанием для принятия мер, регламентирующих доступ в сеть Интернет в ОО (которые включают ограничение доступа обучающихся к ресурсам Интернета, содержащим информацию, не совместимую с задачами образования и воспитания детей; размещение информации на Интернет-ресурсах ОО), являются приказы и письма регионального и (или) муниципального уровней, а также федеральные законы:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Для обеспечения функционирования системы информационной безопасности в ОО, необходим пакет внутренних нормативных документов. Далее рассмотрим документы по направлениям информационной безопасности в ОО.

Защита персональных данных субъектов образовательного процесса

Образовательные организации являются операторами персональных данных, поскольку занимаются обработкой персональных данных учащихся и педагогов. Следовательно, ответственными сотрудниками этих учреждений должен обеспечиваться ФЗ № 152 «О персональных данных».

Статья 19 ФЗ № 152 «О персональных данных». Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Использование и хранение биометрических персональных данных (далее ПДн) вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

В рамках образовательных организаций должен быть выполнен комплекс работ по сбору пакета документов (25 форм), предоставляемых на проверку регуляторам (контролирующим организациям).

Сложность состоит в том, что в настоящее время отсутствуют нормативные акты, утверждающие форму этих типовых ведомственных документов по защите персональных данных в образовательных организациях.

— Пакет документов для проверки;
— положение о защите персональных данных;
— положение о подразделении по защите информации;
— приказ о назначении лиц, ответственных за обработку ПДн;
— концепция информационной безопасности;
— политика информационной безопасности;
— перечень персональных данных, подлежащих защите;
— приказ о проведении внутренней проверки;
— отчет о результатах проведения внутренней проверки;
— акт классификации информационной системы персональных данных;
— положение о разграничении прав доступа к обрабатываемым персональным данным;
— модель угроз безопасности персональных данных;
— план мероприятий по защите ПДн;
— порядок резервирования технических средств и программного обеспечения, баз данных и средств защиты информации;
— план внутренних проверок;
— журнал учета мероприятий по контролю безопасности ПДн;
— журнал учета обращений субъектов ПДн о выполнении их законных прав;
— инструкция администратора информационной системы персональных данных;
— инструкция пользователя информационной системы персональных данных;
— инструкция администратора безопасности информационной системы персональных данных;
— инструкция пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
— перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;
— типовое Техническое задание на разработку системы обеспечения безопасности информации объекта вычислительной техники;
— эскизный проект на создание системы обеспечения безопасности информации объекта вычислительной техники;
— положение об Электронном журнале обращений пользователей информационных систем персональных данных (проект приказа).

Шаблоны документов по защите персональных данных можно скачать по ссылке http://clck.ru/9LWUs. Предоставляется интернет-проектом «Дневник.ру».

Защита информационных ресурсов (ИР), обучающихся от нежелательной информации, антивирусная защита

Для организации безопасного доступа в Интернет, в образовательной организации необходимо разработать следующий пакет документов:

- правила использования сети Интернет в ОО для всех субъектов образовательного процесса;
- документ ознакомления и согласия с Правилами использования сети Интернет в ОО, удостоверенное подписью в документе ознакомления и согласия с правилами. Регулярное (периодичное) заполнение документа ознакомления;
- инструкция для сотрудников ОО о порядке действий при осуществлении контроля за обучающимися, работниками организации, родителями при использовании ресурсов Интернета
- приказ, назначающий администратора точки доступа к сети Интернет;
- должностная инструкция администратора точки доступа к сети Интернет в ОО;
- положение о Совете образовательной организации по вопросам регламентации доступа к ресурсам сети Интернет. В положении указать персональный состав Совета, поддерживать в актуальном состоянии персональный состав Совета;
- регламент работы обучающихся, родителей, учителей (преподавателей) и других сотрудников ОО;
- документ регистрации посетителей точки доступа к сети Интернет в образовательной организации;
- документ регистрации ресурсов, посещаемых с точки доступа к сети Интернет в образовательном учреждении. Регулярное (периодичное) заполнение документов регистрации;
- ответственный за антивирусную безопасность ОО;
- локальные акты, регламентирующие обязанности ответственных за антивирусную безопасность ОО;
- положение «О защите детей от информации, причиняющей вред их здоровью и развитию» в ОО, содержащее классификаторы информации, доступ к которой обучающимся запрещен и разрешен;
- лицензионное соглашение или договор на использование программных контент-фильтров, используемых в ОО;

Напомним, что на всех компьютерных устройствах, входящих в сеть ОО, необходимо установить лицензионное антивирусное программное обеспечение и регулярно обновлять антивирусные базы (сигнатуры), в том числе и на личных устройствах обучающихся и сотрудников.

Организация контентной фильтрации для защиты обучающихся от нежелательной информации

Рассмотрим перечень видов информации, запрещенной к распространению посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Именно данная информация не должна появляться на экранах компьютерных устройств субъектов образовательного процесса в образовательной организации.

№ п/п	Виды информации	Описание видов информации
Информация, запрещенная для распространения среди детей, согласно части 2 статьи 5 Федерального закона № 436-ФЗ		
1.	Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания и/или изображения способов причинения вреда своему здоровью, самоубийства; обсуждения таких способов и их последствий, мотивирующая на совершение таких действий
2.	Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая рекламу или объявления/предложения о продаже наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участии в азартных играх, использовании или вовлечении в проституцию, бродяжничество или попрошайничество, содержащая обсуждение или организующую активность на данную тему
3.	Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных Федеральным законом № 436-ФЗ	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, аудио и видеоматериалы актов насилия или жестокости, жертв насилия и жестокости, участников актов насилия и жестокости, обосновывающие или оправдывающие акты геноцида, военных преступлений, преступлений против человечности, террористических акций, массовых и серийных убийств, содержащие обсуждения участия или планирование совершающихся или будущих актов насилия или жестокости

4.	Отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), призывающая к отказу от семьи и детей («чайлдфри»), страницы клубов для лиц нетрадиционной сексуальной ориентации, сообщества и ресурсы знакомств людей нетрадиционной сексуальной ориентации, содержащая описания, фотографии, рисунки, аудио и видеоматериалы, описывающие и изображающие нетрадиционные сексуальные отношения
5.	Оправдывающая противоправное поведение	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, аудио и видеоматериалы, содержащие призывы к противоправному поведению, одобрение противоправного поведения
6.	Содержащая нецензурную брань	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая нецензурную брань
7.	Содержащая информацию порнографического характера	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио и видеоматериалы по данной теме
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	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, аудио и видеоматериалы по данной теме
Информация, распространение которой среди детей определенных возрастных категорий ограничено, согласно части 3 статьи 5 Федерального закона № 436-ФЗ		
9.	Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме

10.	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	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме
11.	Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая описания, фотографии, рисунки, видеоматериалы по данной теме
12.	Содержащая бранные слова и выражения, не относящиеся к нецензурной брани	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая указанные виды информации
Информация, не соответствующая задачам образования*		
13.	Компьютерные игры, за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет) по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские онлайн родевые игры (MMORPG), массовые многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты
14.	Ресурсы, базирующиеся либо ориентированные на обеспечении анонимности распространителей и потребителей информации	Анонимные форумы, чаты, доски объявлений и гостевые книги, такие как имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети Интернет (tor, I2P)
15.	Банки рефератов, эссе, дипломных работ, за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), представляющая собой банки готовых рефератов, эссе, дипломных работ, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность
16.	Онлайн-казино и тотализаторы	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети Интернет), содержащая информацию об электронных казино, тотализаторах, играх на деньги

17.	Мошеннические сайты	Сайты, навязывающие платные услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг)
18.	Магия, колдовство, чародейство, ясновидящие, приворот по фото, теургия, волшебство, некромантия, тоталитарные секты	Информационная продукция, оказывающая психологическое воздействие на детей, при которой человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние

Для организации защиты детей от вышеобозначенной нежелательной информации в образовательных организациях используются следующие траектории:

1. Использование системы контентной фильтрации (далее СКФ), которая устанавливается на компьютеры и мобильные устройства обучающихся.
2. Заключение с провайдером договора о фильтрации данных, поступающих через браузер на компьютеры в ОО.

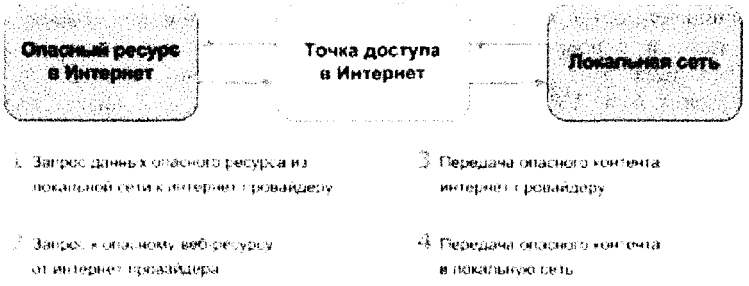
Рассмотрим СКФ, которую поддерживают сотрудники ОО. Средствами контент-фильтрации доступа в Интернет являются аппаратно-программные или программные комплексы, обеспечивающие ограничение доступа к интернет-ресурсам, не совместимым с задачами образования и воспитания обучающихся.

Считаем необходимым, рассмотреть основы работы контент-фильтра. Наиболее широкое распространение получили три алгоритма фильтрации:

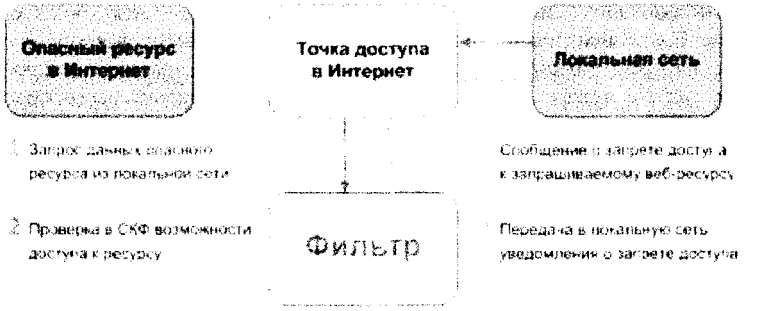
— фильтрация по ключевым словам – конкретные слова и словосочетания используются для включения блокировки веб-сайта.
— динамическая фильтрация – содержимое запрашиваемого веб-ресурса анализируется в момент обращения. Загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное.
— URL фильтрация – запрашиваемая страница или целый домен (например, dosug.nu) могут быть определены или категоризированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется.

Лучшие в мире системы контентной фильтрации используют URL фильтрацию, основанную на анализе и категоризации интернет-ресурсов. Такой механизм признан наиболее эффективным методом фильтрации контента.

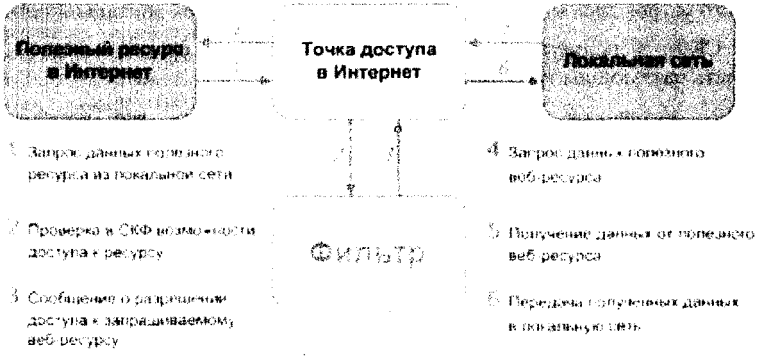
Как работает фильтр? При неуправляемом доступе к интернет-ресурсам запрос от пользователя транслируется через точку доступа в Сеть к любому ресурсу. Пользователь получает запрашиваемую информацию, как показано на рисунке ниже.



При использовании фильтра перед исполнением запроса ресурс проверяется на принадлежность к конкретной категории. Если веб-ресурс принадлежит к одной из запрещенных категорий, то доступ пользователя к такому ресурсу будет блокирован. Схема запрета доступа к опасному ресурсу представлена на рисунке ниже.



Если ресурс не относится к одной из запрещенных категорий, то доступ к ресурсу будет разрешен (см. ниже).



Разрешение доступа к неизвестному ресурсу. Если пользователь запрашивает доступ к ресурсу, не определенному в фильтре, то доступ будет разрешен, и одновременно будет запущен процесс категоризации нового ресурса. Если этот ресурс будет отнесен к категории опасных, то, после обновления базы URL системы, последующие запросы к такому интернет-ресурсу будут заблокированы.

В любой системе фильтрации контента возможны несколько способов отбора информации:

— разрешить только избранные сайты (белый список);
— запретить только избранные сайты (черный список);
— блокировать сайты если на них встречается набор запрещенных слов.

Обычно используется или первый способ, или второй в совокупности с третьим. Но абсолютно защитить обучающихся от нежелательного контента не может ни один из вариантов. Белый список нужно постоянно пополнять, это дополнительные трудовые и временные затраты. Часто при использовании белого списка нужные сайты оказываются блокированными.

Использование черного списка подразумевает запрет некоторых сайтов, что еще более ненадежно, так как ежедневно появляется несколько тысяч сайтов, которые можно назвать вредоносными. Фильтрация по ключевым словам, так же может оказаться не эффективной, поскольку всего просто не предусмотреть, и могут быть заблокированы «добропорядочные» ресурсы.

Необходимо отметить, что СКФ может состоять только из клиентской части или клиентской и серверной части. Первый вариант используется, когда в ОО нет сервера в локальной сети, тогда программное обеспечение устанавливает на все компьютеры ОО, с которыми работают обучающиеся. При необходимости изменения списка СКФ, необходимо настраивать программное обеспечение на каждом компьютере. Такой вариант подходит для небольших школ, с малым количеством устройств. При использовании второго варианта, клиентская часть устанавливается только на компьютеры локальной сети ОО, серверная часть на компьютер-сервер и управление СКФ осуществляется с данного устройства, что облегчает задачу администратора локальной сети.

СКФ, используемые в общеобразовательных организациях, должны отвечать следующим требованиям:

1. Установка СКФ должна производиться на все компьютерное оборудование общеобразовательных организаций, имеющих доступ к Интернету.

2. Обеспечивать беспрепятственный доступ к информации, распространение к которой в Российской Федерации в соответствии с законодательством Российской Федерации не ограничивается или не запрещается.

3. Обеспечить мониторинг использования интернет ресурсов в образовательном процессе в целях обучения и воспитания учащихся.

4. Обеспечить возможность адаптации к изменяющимся угрозам, условиями эксплуатации, требованиям законодательства Российской Федерации предписаниям надзорных органов.

5. Обеспечить фильтрацию контента по спискам категорий, рекомендованным Минобрнауки России и размещенным в сети Интернет на сайте единой системы контент фильтрации доступа к сети Интернет по адресу: http://www.skf.edu.ru.

6. Реализовывать единую политику для всех ОО по исключению доступа к интернет-ресурсам, несовместимым с задачами образования и воспитания обучающихся.

При установке СКФ на устройства ОО направляют уведомление об их подключении по форме регистрации СКФ, размещенной на сайте единой системы контент-фильтрации (skf.edu.ru), а также уведомляют орган исполнительной власти субъекта РФ, осуществляющий управление в сфере образования, об установке СКФ в ОО с указанием количества подключенных устройств, наименования и количества СКФ, используемых в ОО.

Для подключения к единой системе контент-фильтрации доступа к сети Интернет общеобразовательным учреждениям необходимо использовать СКФ, рекомендованную Минобразованием России, либо СКФ, приобретенную самостоятельно.

Предлагаем сравнительный анализ программных продуктов, осуществляющих контент-фильтацию на их соответствие с Правилами подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации

	Характеристики	Интернет цензор	NetPolice pro	Content Keeper	KidGid	ChildWeb Guardian
1	Обеспечивать беспрепятственный доступ к информации, распространение к которой в Российской Федерации в соответствии с законодательством Российской Федерации не ограничивается или не запрещается	+	+	+	+	+
2	Обеспечить возможность адаптации к изменяющимся угрозам, условиями эксплуатации, требованиям законодательства Российской Федерации предписаниям надзорных органов	+	+	+	+	+

3	Обеспечить фильтрацию контента по спискам категорий, рекомендованным Минобрнауки России и размещенным в сети Интернет на сайте единой системы контент фильтрации доступа к сети Интернет по адресу: http://www.skf.edu.ru	+	+	+	-	+
4	Обеспечить мониторинг использования интернет ресурсов в образовательном процессе в целях обучения и воспитания учащихся	+	+	-	-	+
4	Возможность установки на каждый компьютер	Да	Да	Да	Да	Да
5	Тип лицензии	Бесплатно	Платно	Платно	Платно	Платно
6	Сайт программы	www.icensor.ru	www.netpolice.ru	www.contentkeeper.com	www.kidgid.ru	www.childwebguardian.ru

Более подробную информацию о СКФ можно прочитать ниже.

Интернет-цензор (http://www.icensor.ru/). Бесплатный интернет-фильтр для детей. Работает только под Windows и нет возможности централизованного управления для всех компьютеров в сети. Это решение больше подойдет для небольшой группы компьютеров. При установке просит придумать пароль и указать электронную почту для восстановления пароля и отправки уведомлений.

SkyDNS (https://www.skydns.ru/). Российский облачный интернет-сервис, предоставляющий услуги контент-фильтрации. Вся суть в замене DNS-серверов компьютера на предоставленный DNS-сервер компании. Можно указать вручную, или установить программу-клиент с официального сайта, которая сделает все сама, из программы можно выбрать категории фильтрации. Клиент только для ОС Windows. Если клиент не использовать, необходим внешний статический IP-адрес, а также вручную сделать привязку в личном кабинете на сайте.

UserGate Proxy & Firewall (http://usergate.ru/products/usergate/). Представляет собой интернет-шлюз, который устанавливается на отдельный компьютер под управлением Windows. В комплекте идет трехъядерный антивирус, межсетевой экран, контент-фильтр, контроль и мониторинг пользователей и еще несколько полезных функций.

KinderGate (http://usergate.ru/products/kindergate_parental_control/). Контент-фильтр, разработанный компанией Entensys, как и UserGate. Есть клиенты под основные ОС, фильтрация по содержимому сайта, фильтр по категориям, родительский контроль, безопасный поиск, контроль загрузки файлов, поддерживает кластеризацию и фильтрацию HTTPS-протокола.

Интернет Контроль Сервер (http://xserver.ja-read.ru/). Интернет-шлюз, разработанный на базе FreeBSD. Имеет внушительный функционал. В комплекте идут контентная фильтрация, категории трафика SkyDNS, модуль DLP и IP-телефонии, встроенный антивирус, учет трафика и контроль доступа, прокси-сервер, защита корпоративной сети, почта, FTP, Web и Jabber сервер. Явные преимущества этого решения в том, что можно бесплатно использовать полнофункциональную версию на 8 пользователей.

Рассмотрим вариант использования СКФ со стороны провайдера, предоставляющего Интернет ОО. Провайдеры, заключая договор с ОО, автоматически предоставляют фильтрацию ресурсов сети Интернет на низком уровне. Фильтрация на уровне DNS сервера позволяет ограничить доступ к определенным ресурсам, но при этом не учитывается содержимое загружаемых страниц. В данном случае персональная контент-фильтрация считается не установленной, и юридическую ответственность организация-провайдер не несёт. Если ОО заключает договор с провайдером на обслуживание Интернета и желает, чтобы провайдер предоставил персональную контент-фильтрацию в ОО, то в договоре необходимо прописать фразу «... предоставляет персональную контент-фильтрацию и несетответственность за выполнение Федерального закона Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в образовательной организации». Соответственно, стоимость такого пакета услуг повысится, но таким образом, ОО перекладывает всю ответственность за контентную фильтрацию на провайдера. Но в реальности провайдеры используют «белые списки» и тем самым блокируют и полезные ресурсы, а процесс добавления сайтов в список незапрещенных сайтов затягивается.

Кроме того, в общеобразовательных организациях должен реализовываться комплекс мероприятий по обеспечению исключения доступа обучающихся к ресурсам Интернета, содержащим информацию, несовместимую с задачами образования и воспитания, в том числе и с личных устройств. Необходима пропаганда повышения информационной культуры по использованию ресурсов Интернета для всех субъектов образовательного процесса, актуализация вопросов использования программного обеспечения родительского контроля, ограничения времени доступа детей к Интернету.

Система защиты персональных данных участников образовательного процесса

Определение термина «персональные данные» можно найти в двух основных нормативных документах – Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Трудовом кодексе РФ. К персональным данным относится информация, которая позволяет идентифицировать лицо. Единственное отличие определений заключается в том, что трудовое законодательство говорит именно о работниках, закон – о любых субъектах персональных данных.

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ к персональным данным относится любая информация о физическом лице: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. Обработкой персональных данных признаются действия (операции) с ними, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение данных.

Защита персональных данных представляет собой комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Образовательная организация собирает и использует большой массив информации обо всех участниках образовательного процесса. В настоящее время в образовательных организациях активно внедряются информационные системы, осуществляющие обработку персональных данных, делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных обучающихся, родителей и работников, оперативного управления организацией. Вместе с тем, любой гражданин обладает правами на неприкосновенность частной жизни, личную и семейную тайну. Эти права не должны нарушаться ради эффективности образовательного процесса либо удобства работы с персоналом. Одной из задач законодательства, и, следовательно, образовательной организации является охрана и защита персональных данных обучающихся, их законных представителей и работников.

Защита персональных данных участников образовательного процесса в образовательной организации осуществляется на основе следующих нормативно-правовых документов:

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»,

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,

Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»,

документы, регламентирующие вопросы обеспечения безопасности персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 № 21:

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В комплекс мероприятий по защите персональных данных в образовательной организации входят:

– разработка необходимых документов в интересах организации по обеспечению защиты персональных данных;

– обоснование требований по защите информации в информационных системах персональных данных;

– применение методики оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– определение состава и структуры программно-аппаратных средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

Законодательное обеспечение защиты персональных данных

Закон № 152-ФЗ определяет требования к сбору и обработке (хранению, актуализации, использованию, раскрытию и предоставлению) персональных данных физических лиц во всех сферах, где используются персональные данные, в т. ч. в сфере трудовых правоотношений. Требования закона распространяются на все организации (независимо от формы собственности), в т. ч. на образовательные, которые выступают операторами, обрабатывающими в своих информационных системах персональные данные физических лиц (работников, обучающихся и др.).

Вопрос правовой регламентации обеспечения защиты персональных данных работников в настоящее время особенно актуален, поскольку информационные системы персональных данных работников образовательной организации должны представлять собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

В соответствии с частью 3 статьи 4 Закона № 152-ФЗ постановлением Правительства РФ от 15.09.2008 № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Данное Положение предусматривает, что обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований этого Положения.

Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 05.02.2010 № 58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных, которое подробно регламентирует вопросы, связанные с порядком применения методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным им лицом. В соответствии с частью 1 статьи 22 Закона № 152-ФЗ оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять

обработку персональных данных, за исключением случаев, предусмотренных частью 2 указанной статьи.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Россвязькомнадзор) выступает таким уполномоченным органом, который приказом от 17.07.2008 № 08 утвердил образец Уведомления об обработке (о намерении осуществлять обработку) персональных данных и Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных.

Частью 2 статьи 22 Закона № 152-ФЗ установлено, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения. Следовательно, образовательные организации не должны уведомлять этот уполномоченный орган об обработке ими персональных данных работников, состоящих в трудовых отношениях с учреждениями.

Планирование мероприятий по защите персональных данных

При планировании в образовательной организации мероприятий, связанных с защитой персональных данных, рекомендуется привлекать юристов, специалистов отдела кадров по информационной работе (компьютерным технологиям).

Правовая составляющая должна стать обязательным элементом всей деятельности организации в этом направлении, поскольку необходимо:

– разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных;

– сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т. д.

Главным условием защиты персональных данных является четкая регламентация функций работников, а также принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных.

Далее ключевым вопросом становится оценка наличия предусмотренных законодательством оснований для обработки персональных данных, а в случаях, когда они отсутствуют, – получение согласия субъекта персональных данных на их обработку. При этом согласно Закону № 152-ФЗ обязанность доказательства согласия субъекта персональных данных на их обработку возлагается на оператора, т. е. на работодателя.

Несмотря на то, что в данном комментарии речь идет исключительно о защите персональных данных работников, необходимо обратить внимание на то, что ***в образовательной организации обрабатываются персональные данные обучающихся и их родителей, поэтому организация предварительно***

должно получить согласие родителей на обработку персональных данных их самих и их детей.

Следует уделить особое внимание процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие:

– основания для такой передачи, предусмотренные федеральными законами, или согласия субъекта персональных данных, закрепленного, например, в договоре на оказание услуг;

– договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

Необходимо очень внимательно подойти к вопросу размещения информации, содержащей персональные данные на сайте образовательной организации.

С учетом выше изложенного можно выделить следующие обязательные этапы работы по защите персональных данных работников:

1) определение всех ситуаций, когда требуется проводить обработку персональных данных;

2) выделение процессов, в которых обрабатываются персональные данные;

3) выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

4) определение круга информационных систем и совокупности обрабатываемых персональных данных;

5) проведение категорирования персональных данных и предварительной классификации информационных систем;

6) разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

7) внедрение системы обеспечения безопасности информации.

Следовательно, защита персональных данных работников в образовательной организации, по сути, сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;

– организацию системы защиты персональных данных;

– внедрение технических мер защиты персональных данных.

Правовое регулирование вопросов обеспечения защиты персональных данных работников на локальном уровне

В соответствии со ст. 85 ТК РФ к персональным данным работника относится информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Вопрос о том, какая необходимая работодателю информация из категории персональных данных работника подлежит защите, работодатель должен решить самостоятельно с учетом действующего законодательства и с участием самих работников и их представителей.

Статьей 87 ТК РФ предусмотрено, что порядок хранения и использования персональных данных работников устанавливается работодателем с учетом требований ТК РФ и иных федеральных законов, что подразумевает регулирование порядка обработки персональных данных работников локальными нормативными и иными актами.

Основным таким локальным нормативным актом должно быть Положение о защите персональных данных работников, которое принимается с учетом мнения выборного органа первичной профсоюзной организации учреждения в порядке, предусмотренном ст. 372 ТК РФ.

Этот документ определяет: порядок обработки персональных данных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Данный локальный нормативный акт является обязательным, поэтому его отсутствие может быть квалифицировано государственным органом контроля и надзора как нарушение работодателем трудового законодательства.

Наряду с Положением о защите персональных данных работников в образовательной организации также необходимо наличие следующих документов:

– в процессе получения персональных данных – согласие работника на получение работодателем персональных данных от третьих лиц и уведомление работника о получении его персональных данных от третьих лиц*;

– при обработке персональных данных – согласие работника на обработку его персональных данных; персональных данных работников;

– при хранении персональных данных – приказ об утверждении списка лиц, имеющих доступ к персональным данным работников, и обязательств о неразглашении;

– при передаче персональных данных работников – согласие работника на передачу его персональных данных третьим лицам.

Поскольку на работодателя возложена обязанность соблюдения режима конфиденциальности персональных данных, в целях обеспечения его выполнения необходимо вести журналы учета персональных данных, их выдачи и передачи другим лицам и представителям различных организаций, органам контроля и надзора, правоохранительным органам, которые обеспечат документальную фиксацию внутреннего и внешнего доступа к персональным данным работников.

В Журнале учета внутреннего доступа к персональным данным (доступа работников организации к персональным данным других работников) следует указывать такие сведения, как: даты выдачи и возврата документов (личных

дел); срок пользования; цели выдачи; наименование выдаваемых документов. Лицо, которое возвращает документ, содержащий персональные данные, должно обязательно присутствовать при проверке наличия всех имеющихся документов по описи, если выданные документы составлены более чем на одном листе.

Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

Помимо этого необходимо вести журнал учета выдачи персональных данных работников организациям и государственным органам, в котором необходимо регистрировать: поступающие запросы, сведения о лице, направившем запрос; дату передачи персональных данных или уведомления об отказе в их предоставлении; какая именно информация была передана.

Система учета персональных данных может предусматривать проведение регулярных проверок наличия документов и других носителей информации, содержащих персональные данные работников, а также устанавливать порядок работы с ними. В этой связи необходимо ведение журнала проверок наличия документов, содержащих персональные данные работников.

Таким образом, рекомендуется ведение в ОУ следующих учетных документов движения персональных данных работников:

Журнал учета внутреннего доступа к персональным данным работников в учреждении;

Журнал учета выдачи персональных данных работников учреждения организациям и государственным органам (Журнал учета внешнего доступа к персональным данным работников);

Журнал проверок наличия документов, содержащих персональные данные работников.

Кроме того, поскольку к методам и способам защиты информации от несанкционированного доступа для обеспечения безопасности персональных данных в информационных системах определенного класса относится учет всех защищаемых носителей информации (с помощью их маркировки и занесения учетных данных в журналы учета), необходимо также ведение Журнала учета применяемых работодателем носителей информации.

Обязанности работодателя по обеспечению защиты персональных данных работников

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника в соответствии со ст. 86 ТК РФ обязаны соблюдать необходимые требования. В соответствии со ст. 21 Закона № 152-ФЗ оператор (работодатель) также обязан:

1) осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента обращения субъекта персональных данных или его законного представителя либо

получения запроса уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора на период проверки. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;

2) устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления. В случае невозможности устранения допущенных нарушений в указанный срок оператор обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных – также указанный орган;

3) незамедлительно прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты достижения цели обработки, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае поступления обращения или запроса от уполномоченного органа по защите прав субъектов персональных данных – также указанный орган;

4) прекратить обработку персональных данных и уничтожить их, в случае отзыва субъектом персональных данных согласия на их обработку, в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Порядок передачи работодателем персональных данных работников

Персональные данные работника не могут быть переданы работодателем третьей стороне. Исключением из данного правила являются следующие случаи:

– выдача работником письменного согласия на передачу персональных данных третьей стороне;

– передача персональных данных работника в целях предупреждения угрозы жизни и здоровью самого работника;

– другие случаи, установленные федеральным законом.

При передаче персональных данных работника работодатель должен соблюдать следующие обязательные требования, предусмотренные ст. 88 ТК РФ:

– не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами;

– разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

– передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Поскольку персональные данные относятся к категории конфиденциальной информации, лица, получившие персональные данные работника на законном основании, обязаны использовать их исключительно в целях, которые заявлялись при запросе соответствующей информации, а также не разглашать такую информацию (исключения из данного правила определяются только федеральными законами).

Получателями персональных данных работника на законном основании являются:

1) органы социального страхования, органы пенсионного обеспечения, а также иные органы, организации и граждане (в соответствии с Федеральным законом от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования», согласно которому отношения по обязательному социальному страхованию возникают у страхователя (работодателя) – по всем видам обязательного социального страхования с момента заключения с работником трудового договора);

2) налоговые органы (в соответствии со ст. 24 Налогового кодекса РФ, выступая в качестве налогового агента работников, исчисляющего, удерживающего из средств, выплачиваемых работникам, и перечисляющего в бюджет соответствующие налоги, работодатель обязан представлять в налоговый орган по месту своего учета документы, необходимые для контроля за правильностью исчисления, удержания и перечисления налогов);

3) органы прокуратуры и другие правоохранительные органы (в соответствии со ст. 23 Закона № 152-ФЗ они имеют право запрашивать информацию у работодателей в рамках проверки для решения вопроса о возбуждении: дела об административном правонарушении; уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью);

4) федеральная инспекция труда (в соответствии со ст. 357 ТК РФ государственные инспекторы труда при осуществлении надзорно-контрольной деятельности имеют право запрашивать у работодателей и безвозмездно

получать от них документы и информацию, необходимую для выполнения надзорных и контрольных функций, включая персональные данные работников);

5) профессиональные союзы (в соответствии с Федеральным законом от 12.01.1996 № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» и ТК РФ профсоюзы имеют право на получение информации от работодателей по социально-трудовым вопросам для осуществления своей уставной деятельности, а также на осуществление общественного контроля за соблюдением работодателями, должностными лицами трудового законодательства);

6) другие органы и организации в случаях, предусмотренных федеральным законом.

Права и обязанности работников, связанные с обработкой и защитой их персональных данных

В соответствии с п. 8 ст. 86 ТК РФ работники и их представители должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки и защиты персональных данных, а также их права и обязанности в этой области. Работники в соответствии со ст. 89 ТК РФ имеют право:

– на полную информацию о своих персональных данных и обработке этих данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

– на определение своих представителей для защиты персональных данных;

– на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

– на требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– на требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– на обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Работники обязаны в разумный срок информировать работодателя об изменении персональных данных.

Ответственность за нарушение требований по защите персональных данных

В соответствии со ст. 24 лица, виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность Закона № 152-ФЗ.

Неисполнение требований Закона № 152-ФЗ операторами баз данных может повлечь:

– гражданские иски со стороны работников;

– репутационные риски;

– приостановление или прекращение обработки персональных данных, осуществляемой с нарушением требований Закона № 152-ФЗ;

– направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных;

– привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях.

В соответствии со ст. 90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

Так, к работнику, отвечающему за хранение персональных данных в силу его трудовых обязанностей, работодатель вправе применить одно из дисциплинарных взысканий, предусмотренных ст. 192 ТК РФ (замечание, выговор, увольнение).

Работодатель может расторгнуть трудовой договор по своей инициативе по подп. "в" п. 6 ч. 1 ст. 81 ТК РФ при разглашении работником охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в т. ч. в случае разглашения персональных данных другого работника.

Помимо этого работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к материальной и уголовной ответственности.

Система государственного надзора и контроля в области персональных данных

Система государственного надзора и контроля в области персональных данных строится на функционировании трех регуляторов, ответственных за определенные области деятельности в сфере персональных данных.

Основным регулятором, осуществляющим контроль и надзор за соответствием обработки персональных данных требованиям законодательства РФ в этой области, является уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), территориальные органы которой действуют в каждом субъекте РФ. Зона ответственности и область проверок этого регулятора – все организационные мероприятия, включая акт классификации информационных систем персональных данных. Права и обязанности этого уполномоченного органа устанавливаются положением о нем в соответствии со ст. 23 Закона № 152-ФЗ.

Вторым регулятором, контролирующим осуществление мер по технической защите информационных систем обработки персональных данных, является Федеральная служба по техническому и экспортному контролю (ФСТЭК) и ее территориальные органы. Сфера ответственности и область проверок – технические средства защиты информации, использующие некриптографические методы и способы защиты персональных данных.

Третьим регулятором является федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, – Федеральная служба безопасности РФ (ФСБ России), которая устанавливает особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах и осуществляет контроль в этой области.

Кроме того, следует иметь в виду, что в соответствии со ст. 354 ТК РФ Федеральная инспекция труда, состоящая из федерального органа исполнительной власти и его территориальных органов (государственных инспекций труда), является уполномоченным органом на проведение государственного надзора и контроля за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, в т. ч. и по вопросам защиты персональных данных работников.

Таким образом, тема защиты персональных данных субъектов образовательного процесса в настоящее время особенно актуальна, так как активное использование средств компьютерной техники и информационно-обрабатывающих технологий, а также увеличивающийся объем массивов информации вызывает появление новых правовых проблем, требующих от образовательной организации принятия адекватных мер реагирования.

Организация антивирусной защиты компьютеров и мобильных устройств сети образовательного учреждения (организации)

Для любого активного пользователя сети Интернет вопрос о защите и безопасности электронной информации стоит на первом месте и любое образовательное учреждение не исключение. Все, что содержится на компьютерах, планшетах или мобильных устройствах может быть украденным и удаленным различными вредоносными программами в считанные секунды. Рассмотрим основные виды вредоносных программ.

Компьютерные вирусы – это вредоносный код или вид компьютерных программ, который направлен на то, чтобы нанести вред компьютеру пользователя, похитить или удалить его информацию либо удалённо управлять компьютером в корыстных целях. Таким образом, любая из перечисленных целей вируса – нанести существенный урон компьютеру и парализовать его работу.

Компьютерный червь – это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Известным видом вредоносных вирусных программ являются «трояны». Троянские программы, как правило, маскируются под безвредные программы, чтобы спровоцировать пользователя их запустить. Конечной целью троянской программы является нанесение вреда компьютеру пользователя, как в корыстных, так и бескорыстных целях. Есть такие «трояны», цель которых стереть информацию на жёстком диске компьютера, то есть, все ваши данные: музыку, документы, фильмы, фотографии – всё это удалиться и восстановить их будет практически невозможно. Ещё один вид «троянов» – это хищение сохранённых на компьютере паролей в различных программах, чаще всего хищение паролей происходит из браузеров, таким образом, если это произойдёт, то вы потеряете доступ к своей электронной почте, социальным сетям и другим аккаунтам. Ну и последний распространённый вид троянских программ – которые блокируют работу компьютера с целью получения денежных средств за разблокировку. Иными словами, вы включаете компьютер и у вас появляется окно блокировки, с требованием перечислить определённую сумму денежных средств для разблокирования компьютера.

Помимо этого, есть ещё большое количество видов вредоносных объектов, которые вредят компьютеру, но на них подробно мы останавливаться не будем, можно посмотреть их перечень и основные характеристики в приложении. Мы остановились только на тех, которые реально являются угрозой для школьных

компьютеров. Следовательно, необходимо предусмотреть способы защиты. Таким способом является антивирусная программа.

Антивирусная программа (антивирус) – это специальная программа для обнаружения компьютерных вирусов, а также нежелательных программ, умеющая восстанавливать (лечить) зараженные программы и файлы. Новые системы обнаружения современных антивирусов быстро предотвращают заражение файлов или операционной системы вредоносным кодом.

Кроме защиты компьютера от вирусов и троянских программ, антивирус также может контролировать посещаемые вами сайты, в первую очередь блокировать те ресурсы, которые способны нанести урон вашему компьютеру, попросту это те сайты, на которых есть вирусы. Кроме того, антивирусы могут блокировать рекламу на сайтах, а также всплывающие баннеры, что действительно очень полезно.

Нельзя не отметить такую дополнительную функцию, в некоторых антивирусах, как «родительский контроль». Данная функция предназначена для того, чтобы защитить детей от посещения нежелательных ресурсов в Интернете, и по сути выполняет функции контентного фильтра, с довольно гибкими настройками.

Заразиться вирусной программой можно только извне, то есть, сам по себе вирус в компьютере появиться не может. Существует два варианта заражения компьютера вирусами: через Интернет или через съёмный носитель. Через Интернет ваш компьютер может заразиться вирусом при скачивании каких-либо файлов или же при посещении вредоносных сайтов. Что касается съёмных носителей, то примером таких носителей являются флешки или CD/DVD диски, когда они были записаны на инфицированном компьютере и путём копирования или запуска вируса переместились на ваш компьютер. Антивирусная программа в обоих этих случаях защищает компьютер от попадания вирусов извне.

Сегодня на рынке антивирусных программ сосредоточен большой спектр антивирусов: от самых простых – бесплатных, до мощных – комплексных, где используются лучшие технологии безопасности для защиты разного вида устройств. Какой выбрать антивирус для образовательной организации? Прежде всего, такой, который обеспечит полный комплекс защиты с учетом особенностей и потребностей Вашей школы. Поэтому, какой именно выбрать антивирус – решать Вам. Мы же, в свою очередь, дадим вам критерии для выбора антивирусной программы и перечислим наиболее популярные из них, которые достойны вашего внимания.

Давайте рассмотрим функции антивируса, которые необходимы для надёжной защиты компьютера, в порядке важности:

Антивирусный монитор производит мониторинг файлов и папок с которыми вы работаете, для проверки их на наличие вирусов.

Сканер – это функция, которая осуществляет сканирование жёсткого диска и оперативной памяти, на наличие вирусов. Очень полезная функция чтобы

проверить подозрительные и потенциально опасные файлы на вашем компьютере, особенно полезен сканер для проверки сменных носителей.

Самозащита антивируса. Функция самозащиты антивируса направлена на то, чтобы антивирус мог самостоятельно защитить себя от воздействия вирусов. Существуют вирусы, которые пытаются отключить как некоторые функции антивируса, так и предотвратить его работу в целом, чтобы он не мешал распространятся вирусам по всему компьютеру, именно для этого и нужна функция самозащиты.

Контроль активности программ. Данная функция антивируса направлена на то, чтобы контролировать работу программ. В случае, если программа будет заражена вирусом, то он начнёт вносить изменения в её работу, что должен сразу обнаружить данный контроль антивируса.

Сетевой контроль и веб-антивирус. Эти компоненты антивируса обеспечивают безопасность работы в Интернете. Сетевой контроль контролирует сетевую активность, а веб-антивирус проверяет HTTP-трафик, блокируя угрожающие безопасности компьютера скрипты размещённые на сайтах.

Постоянное обновление антивирусных баз. Очень важной для надёжной защиты антивируса является возможность постоянного обновления антивирусных баз. Антивирусные базы – это своего рода знания о вирусах и их особенностях, которые антивирус использует для обнаружения и предотвращения вирусов. Ввиду того, что новые вирусы появляются чуть ли не каждый день, разработчики антивирусов, при обнаружении нового вируса, должны обучить свои продукты, которые установлены у пользователей, знаниям об их обнаружении и устранении. Таким образом, если вы хотите, чтобы ваш антивирус защищал компьютер не только от известных старых вирусов, но и от новых, обновления должны быть регулярными.

Низкое ресурсопотребление. Одна из проблем многих антивирусов – большое ресурсопотребление. При выборе антивирусного программного обеспечения старайтесь выбрать такой продукт, который не будет сильно нагружать систему, так как в противном случае работать за таким компьютером или ноутбуком будет очень некомфортно.

Репутация и популярность антивируса – очень важный фактор, который необходимо брать во внимание при выборе антивирусной программы. Чем популярнее антивирус, тем соответственно и больше пользователей его используют, а стало быть, вряд ли большое количество людей будут использовать ненадёжный антивирус.

Каждый из нас понимает, что платная продукция всегда имеет лучшее качество, нежели бесплатная. Подумайте: для того, чтобы антивирус надёжно защищал, необходим штат сотрудников, который постоянно будет собирать информацию о новых вирусах и вредоносных кодах с просторов Интернета, а также работать над их нейтрализацией. Затем, данные базы знаний необходимо сформировать в обновления и загрузить их на сервер, чтобы клиентские программы обновились – и так должно быть постоянно. Кроме того,

необходимо заниматься разработкой новых версий и функций антивируса. Какой вывод можно сделать из этого? Для создания и поддержки антивируса необходим целый штат сотрудников и полная их занятость, а стало быть, чтобы это всё организовать, конечный продукт должен покрывать все расходы на данную деятельность. Ну а кто согласится работать за бесплатно? А если вдруг и так, то и качество такого антивируса будет соответствующим.

Рассмотрим основные критерии, предъявляемые к качеству антивирусной программы.

Надежность работы антивируса и простота использования являются наиболее важными критериями, поскольку даже «абсолютный антивирус» может оказаться абсолютно бесполезным, если он конфликтует с системой, резко уменьшает её производительность или периодически «зависает». Если же антивирус требует наличия специальных знаний, которыми не обладает большинство обычных пользователей, то с ним будет слишком сложно работать. Если же корпоративная версия антивируса не содержит необходимого функционала для администрирования сети, то большинство системных администраторов предпочтут менее надёжный, но более удобный продукт.

Комплексность защиты — второй критически важный критерий. Под постоянным контролем должны находиться все области компьютера, все типы файлов, все элементы сети, которые могут стать объектом вирусной атаки. При этом необходимо умение обнаруживать вредоносный код и во всех каналах его возможного проникновения (почта, WWW, FTP и т.д.), защитить все «двери», ведущие внутрь компьютера и компьютерной сети.

Качество защиты является третьим ключевым критерием. Любой самый «навороченный» по своим возможностям антивирус бесполезен, если он не в состоянии обеспечивать достаточный уровень защиты от вредоносных программ. Антивирусам приходится противостоять достаточно агрессивной среде, которая постоянно совершенствуется — часто новые версии вирусов, червей, троянских программ становятся значительно более сложные, чем их предшественники.

Качество же защиты складывается из следующих характеристик продукта: уровень детектирования вредоносных программ, частота и регулярность выхода обновлений, возможность корректного удаления вирусного кода из системы, ресурсоёмкость, возможность использования двойной защиты от разных производителей, умение защищать не только от уже известных — но и от новых вирусов и троянских программ.

Какую именно антивирусную программу установить на компьютер или ноутбук – решать исключительно вам. Далее мы перечислим самые популярные антивирусные программы, которые существуют на сегодняшний день, кратко описав их преимущества и недостатки.

Антивирус Касперского. Пожалуй, самый популярный на сегодняшний день антивирус, который создан и производится в России. Данная антивирусная программа имеет несколько версий, но самыми популярными являются Антивирус Касперского и Kaspersky Internet Security. Отличия этих двух

продуктов, друг от друга, заключаются в том, что Kaspersky Internet Security, помимо антивирусной защиты, которую включает в себя Антивирус Касперского, имеет интернет-защиту, что очень важно для безопасной работы во Всемирной паутине.

Из преимуществ данной антивирусной программы можно отметить высокую степень защиты компьютера, широкий спектр функций и гибкие настройки. К недостаткам «Касперского» можно отнести высокую стоимость лицензии и излишний контроль программы в некоторых аспектах.

Kaspersky Anti-Virus. Защита от вредоносных программ. В Kaspersky Anti-Virus входят новейшие технологии защиты от основных вредоносных программ, в том числе от эксплойтов, использующих уязвимости в операционной системе и приложениях. Проверка репутации программ. Функция позволяет вам мгновенно проверить безопасность любого исполняемого файла на своем компьютере. Актуальная информация о репутации программы поступает в режиме реального времени из «облака».

Модуль проверки ссылок. Вы можете убедиться в безопасности любого сайта, на который собираетесь перейти. Ссылки на подозрительные и опасные ресурсы автоматически помечаются специальным цветовым индикатором. Высокая скорость работы. Благодаря облачным технологиям защиты, интеллектуальному сканированию и компактной установке обновлений работа антивируса на вашем компьютере практически незаметна.

Гибридная защита мгновенно реагирует на новые угрозы. Защита от эксплойтов не позволяет вредоносным программам использовать уязвимости в системе и приложениях. Режим Безопасных программ разрешает запуск только доверенных приложений и ограничивая работу всех подозрительных программ. Мета-сканер проверяет файлы на наличие фрагментов вредоносного кода, характерных для вредоносных программ-эксплойтов, использующих уязвимости в системе и приложениях.

Мониторинг активности выявляет подозрительные действия программ и позволяет отменить вредоносные изменения. Модуль проверки ссылок блокирует опасные веб-сайты. Анти-Фишинг обеспечивает защиту ваших личных данных. Диск аварийного восстановления позволяет восстановить систему в случае заражения.

Инструмент Менеджер паролей генерирует надежные пароли, безопасно хранит пароли в зашифрованном виде и выполняет автоматический вход на сайты и в приложения. А новая возможность хранить пароли в «облаке» позволяет синхронизировать пароли на нескольких компьютерах.

Функции резервного копирования и восстановления данных помогут защитить ценные фотографии, музыку и финансовые документы: в случае порчи жесткого диска, утери или кражи компьютера они по-прежнему будут доступны. Вы можете хранить резервные копии в онлайн-хранилище и иметь доступ к ним с любого компьютера, имеющего подключение к Интернету.

Для хранения ценной информации можно создавать специальные зашифрованные хранилища и защитить их паролем. Хакеры и злоумышленники

не смогут получить доступ к зашифрованной информации, а вы сможете безопасно переносить конфиденциальные данные с одного компьютера на другой.

Инструмент Родительский контроль позволяет управлять доступом детей к компьютеру, Интернету, программам, играм и веб-сайтам, блокировать, ограничивать или отслеживать использование служб мгновенных сообщений и социальных сетей. Более того, вы можете легко контролировать загрузку файлов и даже блокировать передачу личных сведений.

Отдельно стоит отметить антивирус Касперского. Яндекс-версия. Воспользоваться бесплатной шестимесячной лицензией можно только один раз.

Dr.WEB. Второй по популярности антивирус, производимый в России – Dr.Web. Dr.Web также имеет две версии: простой антивирус – Антивирус Dr.Web и версию антивируса + защиту для работы в интернете Dr.Web Security Space.

К большому сожалению, антивирус Dr.Web немного проигрывает на фоне «Касперского», как по количеству функций, так и по защите от вирусов. Тем не менее, Dr.Web используют большое количество пользователей, которые в полной мере довольны его работой, а это очень важный показатель.

АвастAvast! Free Antivirus. Бесплатный чешский антивирус, который пользуется большой популярностью у пользователей как отличный вариант бесплатного антивируса. Если вы не знаете, какой бесплатный антивирус выбрать, то Avast! самый оптимальный антивирус для этих задач. Кроме того, у данного антивируса есть и платные версии, но на них заострять ваше внимание мы не будем.

NOD32. Известный словацкий антивирус, выпускаемый с 1987 года. NOD32 позиционируется как достаточно надёжный антивирус, потребляющий малое количество системных ресурсов и имея высокую скорость антивирусной проверки. По функциям ESET NOD32 Smart Security не отстаёт от своих платных аналогов и включает в себе антивирус и интернет-защиту.

NANO антивирус – российская разработка, на период бэта-тестирования, разработчики предоставляют продукт абсолютно бесплатно.

Comodo Antivirus – мощный пакет комплексной защиты (антивирус, Firewall, модуль защиты), имеет русский интерфейс.

Panda – разработан для защиты системы из «облака» (вычислительные мощности расположены на удаленных серверах, в результате программа практически не загружает компьютер).

Отдельно следует выделить бесплатные антивирусные программы. Нельзя использовать любые «бесплатные» антивирусы в образовательных организациях. В лицензионных соглашениях практически всех антивирусов четко сказано, что они только для домашнего (частного) и при этом некоммерческого использования. Это значит, что для офисов, школ, любых других организаций этот антивирус не годится. Прямое пояснение можно посмотреть на страничке скачивания бесплатного антивируса Avast.

При покупке антивирусных программ образовательной организацией, необходимо искать, так называемые «корпоративные» предложения для системы образования. Некоторые компании продают свои продукты образовательным организациям с большой скидкой. Например, лаборатория Касперского со скидкой до 80%. Dr.Web так же предлагает комплекты по специальным ценам.

Какой антивирус лучше? У каждого из них есть как свои преимущества, так и свои недостатки. Кроме этого, 100% надёжного антивируса нет, любой из них может пропустить вирус, но у кого-то эта вероятность высока, а у кого-то сводится к минимуму. Также, работа самого антивируса и его новых версий может вызывать нарекания, в виду потребления большого количества системных ресурсов и прочих недоработок.

Заключение

В данных методических рекомендациях были рассмотрены механизмы для реализации следующих направлений информационной безопасности в образовательных организациях общего и среднего профессионального образования:

- организация контентной фильтрации данных из Интернета на компьютерных устройствах используемых учениками;
- обеспечение антивирусной защиты и других интернет-угроз компьютеров и мобильных устройств локальной сети организации;
- обеспечение защиты персональных данных субъектов образовательного процесса;
- организация правомерного использования объектов авторского права.

Рассмотрены вопросы разработки системы информационной безопасности ОО, подготовки пакета внутренних нормативных документов и инструкций для функционирования системы информационной безопасности, выбора и организации работы контентной фильтрации, антивирусных программ на компьютерных устройствах сети ОО, разработки системы защиты персональных данных субъектов образовательного процесса, разработки системы защиты информационных ресурсов ОО, проведение мероприятий с участием субъектов образовательного процесса для повышения уровня информационной культуры в области информационной безопасности.

Данные методические рекомендации позволят оптимизировать процесс обучения на программах повышения квалификации, где рассматриваются вопросы информационной безопасности образовательной организации, а также окажут методическую помощь педагогам-практикам в создании, усовершенствовании системы информационной безопасности образовательной организации в соответствии с существующими нормативно-правовыми документами.

Ждем предложений по изменению методических рекомендаций по электронным адресам авторов: Н.Ю. Сероштанова – seroshtanova@gmail.com, Е.В. Тюгаева – tugaeva@gmail.com, Н.В. Шпарута – shparuta@gmail.com.

Глоссарий

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную

систему персональных данных и / или выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и / или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записи ключей и атрибутов доступа (паролей) на бумажные носители и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Список рекомендуемой литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М. : Академия, 2006. – 256 с.
4. Партыка Т.Л., Попов И.И. Информационная безопасность. – 2-е изд. – М. : ФОРУМ : ИНФРА-М, 2007. – 368 с.
5. Защита информации в вычислительных системах // под. ред. Храмова В.В. – М. : ПНЦ РАН, 2002. – 318 с.
6. Закупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. – 2009. – №4.
7. Шубинский М.И. Информационная безопасность для работников бюджетной сферы : учеб. пособие / НИУ ИТМО. – СПб., 2012.
8. Шафеева Е.Ю. Шубинский М.И. Основы безопасности жизнедеятельности в сети Интернет (ОБЖИ) : метод. пособие / МПСС. СПб., 2010.
9. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет. М., 2004. URL: http://www.ioso.ru/distant/library/publication/infobez.htm (режим доступа 28.01.2014)
10. Петров В. СМИ как информационное оружие // ОБЖ. Основы безопасности жизни. – 2008. – № 3. – С. 48-54.
11. Жукова М.В. Увлечение компьютерными играми как фактор формирования зависимого поведение в дошкольном возрасте // Начальная школа плюс до и после. – 2010. – № 10. – С. 32-36
12. Шишова Т. В плену у «умного ящика» // Народное образование – 2002. – № 8. – С. 176-182
13. Богатырев А.Н. О применении компьютерных игр в учреждениях дополнительного образования // Дополнительное образование. – 2001. – № 9. – С. 52-62
14. Эльмаа Ю. Компьютерные игры: детская забава или педагогическая проблема? // Директор школы. – 2003. – № 9. – С. 36-40
15. Тулахонова М. Проблема информационной безопасности школьников // Народное образование. – 2009. – № 6
16. Малых Т.А. Информационная безопасности школьников // Спутник классного руководителя. – 2010. – № 3
17. Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания. — М.: МегаВерсия, 2006.