**Семинар-практикум**

**«Безопасность в информационном обществе»**

*Цель программы семинара-практикума:* формирование участников семинара-практикума компетенций необходимых, для создания безопасной информационной среды в образовательных организациях Курчатовского района

*Задачи:*

1. Изучить содержание нормативно-правовых документов по вопросам безопасности персональных данных.
2. Определить понятие «персональные данные»
3. Сформировать понятийный аппарат по вопросам защиты персональных данных
4. Сформировать представление об основных механизмах защиты персональных данных
5. Дать методические рекомендации для работы со всеми участниками образовательных отношений

*Форма проведения:* семинар-практикум, очная

*Методы проведения:* интерактивная лекция, доклады, практические занятия

*Аудитория*: педагогический коллектив

*Продолжительность*: 2 ч.

*Планируемый результат:* Участники семинара-практикума изучат содержание нормативно-правовой базы по теме, овладеют понятийным аппаратом по вопросам безопасности персональных данных, приобретут навыки трансляции полученных компетенций для всех участников образовательных отношений, используя различные формы и методы обучения.

После семинара педагоги будут:

Знать:

1. основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
2. основные понятия и термины в области персональных данных;
3. меры обеспечения безопасности персональных данных;
4. методы организации работы с персональными данными;
5. требования по обеспечению безопасности персональных данных;
6. формы ответственности за нарушения законодательства.

Уметь:

1. правильно оформлять согласия на обработку персональных данных в соответствии с требованиями законодательства РФ;
2. определять состав и содержание мер по обеспечению безопасности персональных данных.

Владеть:

1. навыками работы с правовыми базами данных;
2. навыками определения уровней защищённости персональных данных;
3. навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных.

Содержание программы семинара-практикума

«Безопасность в информационном обществе»

*Раздел 1. Теоретические основы*

«Безопасная информационная среда образовательной организации, система работы, нормативно-правовая документация, зоны риска» - С.С.Лебедева

 «Персональные данные и их защита в сети Интернет» - Н.П. Жадько

*Раздел 2. Практикум*

 «Роль классного руководителя в обеспечении безопасной информационной среды»- О.П.Кайсарова

«Как помочь ребенку избежать опасности подстерегающие в сети Интернет» - Н.В.Безобразова

«Кибербулинг» - В.П. Черникова

**Раздел 1. Теоретические основы**

**Слайд 1**

Здравствуйте, уважаемы коллеги!

Мы рады приветствовать вас на семинаре-практикуме «Безопасность в информационном обществе».

Слово для преведствия передаётся С.Б. Хайдукову

**Слайд 2**

(Приветственная речь )

**Слайд 3**

**Актуализация темы «Информационная безопасность»**

*С.С.Лебедева, заместитель руководителя по воспитательной работе МБОУ «СОШ №45 г.Челябинска»*

Стремительное развитие современных телекоммуникационных и информационных технологий привело к становлению нового общества – информационного. Использование информационных технологий значительно изменяет не только то, как производятся продукты и услуги, но и то, как все мы живем. С 2014 года утверждена программа на государственном уровне о стратегии развития информационного общества.

**Слайд 4**

* Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»
* Постановление Правительства РФ от 15 апреля 2014 г. N 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)»
* Государственная программа Челябинской области «Развитие информационного общества в Челябинской области на 2016 - 2018 годы» (с изменениями на 20 июня 2018 года) (ПОСТАНОВЛЕНИЕ от 17 ноября 2015 года N 571-П)

Сегодня термины информационное общество и информатизация прочно заняли свое место, причём не только в лексиконе специалистов в области информации, но и в лексиконе политических деятелей, экономистов, преподавателей и ученых.

Технологическая составляющая общественного и экономического развития государств сегодня очень существенна, при этом скорость происходящих под ее воздействием изменений настолько велика, что даже на глазах одного поколения происходит несколько циклов технологического обновления. Актуальное вчера, сегодня уже теряет своё значение.

Каждый из нас уже не представляет жизнь без информационных технологий.

Обратите внимание на слайды! Что сзесь представлено?

**Слайд 5**

 В контакте  Одноклассники



 Инстограмм Фэйсбук



 Твитер Ютюб

 Это популярные онлайн ресурсы. А что они нам дают? Общение и пр. Но самое основное они «сливают» все наши данные, которые мы сами размещаем в соцсетях о себе.

**(Демонстрация видеоролика «Персональные данные»)**

Интернет сегодня является самым востребованным кластером у большинства населения планеты, что вызывает определенные сомнения по поводу безопасности в сети.

Современная жизнь в век информационных технологий диктует нам новые угрозы, о которых ранее никто не задумывался.

**Слайд 6**

Мы не можем не замечать, что стираются границы между абстрактной критерией «информация» и носителем этой информации. Виртуальный мир в современных реалиях представляет угрозу личности, собственности, общественному порядку и государственной безопасности. Так защита той или иной информации может быть приравнена к защите её материального эквивалента.

Обеспечение информационной безопасности требует от каждого человека внимательного отношения, так как даже сделки, касающиеся покупки бытовой техники либо мебели, постепенно переходят в сеть, а сохранение своих сбережений в сложной системе связано с большим объемом рисков. Безопасность в сети интернет необходима для организации конфиденциальности сделок и частной переписки, которая может быть перехвачена в случае некачественного контроля со стороны пользователя. Интернет служит для заключения сделок и покупок, а также для получения информации, поэтому среднестатистическому жителю обходиться без глобальной паутины трудно.

В интернете кроются и отрицательные моменты, которые не дают возможности обеспечить качественную защиту личных данных: Большинство информации в интернете предоставляется без цензуры с расчетом на широкую аудиторию;

Моментальное распространение вирусов через сеть;

Невозможность проследить исходящие данные с дальнейшей их корректировкой;

Официальная регистрация пользователей не является обязательной, что приводит к возможности скрыться после совершения мошенничества;

**Слайд 7**

Кибермошейничество:

**Слайд 8,9,10,11**

Фишинг,фармин, вишинг, смишинг, нигирийские письма, интернет-аукционы, хайп и пр.

Преступления, совершенные в интернете, не всегда можно классифицировать, поэтому привлечь к ответственности за них достаточно сложно. Наличие всех этих факторов заставляет пользователей задумываться о самостоятельном решении проблем, а также применять программы, которые будут отвечать за безопасность информации.

**Слайд 12**

В настоящее время объективной реальностью является необходимость обеспечения безопасности личной информации, поскольку информация о человеке сегодня превратилась в дорогой товар. Защита личной информации может приравниваться к защите личности, при этом степень угрозы безопасности личности (частная жизнь, личная, семейная тайна, жизнь и здоровье личности, собственность и пр.) может определиться в каждом конкретном случае незнакомого использования информации о личности

Для решения проблем защиты участников сети была создана 4 года назад специальная организация – Лига безопасного интернета. Цель деятельности данного объединения заключается в противодействии хакерским атакам, а также в распространении программ контроля над популяризацией в интернете запрещенного видео. Лигу учредили с надеждой на решение глобальных проблем сети, связанных с распространением вирусных ботов и незаконного контента.

А также на государственном уровне сформирована Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Но прежде всего мы должны сами себя защищать в информационном обществе, знать свои права и обязанности в донному направлению, то есть нормативно – правовую базу

**Слайд 13**

«У того, кто решит изучать законы,

не останется времени их нарушать»

И.В. Гете

 В современном мире к информационной безопасности относятся очень серьезно, особенно к защите персональных данных. Нормативные акты, регулирующие обеспечение их сохранности предусмотрены не только национальным законодательством, но и международными актами, например, Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948) является одним из важнейших документов в истории человечества. Статья 12 Всеобщей декларации прав человека 1948 года гласит:

**Слайд 14**

Статья 12 «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

**Слайд 15**

Сохранность персональных данных обеспечивается следующими нормативными актами Российской Федерации: Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

В ее положениях признается не только само право на неприкосновенность личной жизни, личную и семейную тайну (ч.1 ст.23), но и обеспечивающие это право дополнительные гарантии (ч.2 ст.23) (все эти права можно рассматривать как право на приватность). В соответствии со ст. 2 Конституции «человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства».

 Таким образом, Российская Федерация не только устанавливает право, но и обязуется защищать его; ставит интересы человека и гражданина на ступень выше, чем интересы государства, общества, либо общественных или коммерческих организаций. Ч.1 ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. И,наконец, согласно ст. 46 каждому гарантируется судебная защита его прав, в том числе в межгосударственных органах.

Ст. 2 Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства.

Ст. 23 1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Ст. 24 Конституции РФ в действующей редакции на 2018 год:

ч.1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

 [Гл. 2](https://www.zakonrf.info/konstitucia/gl2/) Ст. 46. 1. Каждому гарантируется судебная защита его прав и свобод.

2. Решения и действия (или бездействие) органов государственной власти, органов местного самоуправления, общественных объединений и должностных лиц могут быть обжалованы в суд.

3. Каждый вправе в соответствии с международными договорами Российской Федерации обращаться в межгосударственные органы по защите прав и свобод человека, если исчерпаны все имеющиеся внутригосударственные средства правовой защиты.)

**Слайд 16**

Кроме того, данную сферу регулирует Федеральный закон от 25.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации».В частности, ч.1 ст. 11 Федеральный закон от 25.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» определяет, что персональные данные являются конфиденциальной информацией, а ч.3 этой же статьи предупреждает о наступлении ответственности юридических и физических лиц за нарушение режима защиты, обработки и порядка использования этой информации.

Ст. 11. Информация о гражданах (персональные данные)

ч 1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.

ч 3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации) и соответствующим перечнем, дает им следующее определение:

1. Понятие персональных данных

**Слайд 17**

Для начала необходимо определиться, что такое персональные данные? В Федеральном законе от 25.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации».

Ст.2. Термины, используемые в настоящем Федеральном законе, их определения: информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. В соответствии со ст. 3:Основные понятия, используемые в настоящем Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», они понимаются еще шире. Основу этого Закона составляют базовые принципы и условия обработки персональных данных

Статья 3. Основные понятия, используемые в настоящем Федеральном законе. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Слайд 18**

Такое широкое толкование позволяет относить к персональным данным практически любую информацию о человеке: сведения о его ФИО, поле и возрасте, образовании, месте жительства, семейном положении и др. Помимо этого к персональным данным относится и изображение человека, с помощью которого можно установить его личность – например, фотография, видеозапись или портрет (разъяснения Роскомнадзора от 30 августа 2013 г. «[Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки](http://base.garant.ru/70442932/)»), а также биометрические персональные данные - физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных.

**Слайд 19**

В настоящее время закон от 25.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» не действует, его заменил Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

В ст.2 нового закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) рассмотрены основные понятия, используемые в данном законе, а в ст. 3 говорится о правовом регулировании отношений, возникающих в сфере информации, информационных технологий и защите информации. В этой статье говорится о том, что ограничения доступа к информации может устанавливаться только федеральным законом. Конкретного понятия персональных данных в этом законе нет, очевидно, потому что был утвержден Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

В статье 5 ФЗ «Об информации, информационных технологиях и защите информации», сказано: «информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)».

Общедоступная информация – это та информация, которую нельзя скрывать от общества. Примером может служить информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Информацией ограниченного доступа является информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании. В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную тайну и информацию, соблюдение конфиденциальности которой установлено федеральным законом (конфиденциальная информация).

**Слайд 20**

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015) (информация о частной жизни гражданина отнесена к сведениям конфиденциального характера, следовательно, разглашению и несанкционированному сбору не подлежит).

К видам конфиденциальной информацииможно отнести следующее:

* Персональные данные - сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* Тайна следствия и судопроизводства - сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации;
* Служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
* Профессиональная тайна - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);
* Коммерческая тайна - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
* Сведения о сущности изобретения - сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

2. Обработка персональных данных, их хранение и использование

**Слайд 21**

Все персональные данные на конкретного человека могут быть подвергнуты необходимой обработке (например, формирование списков обучающихся в организации, сотрудников, по полу, возрасту, профессии, образованию и т.п.; подготовка работодателем списков работников, подлежащих медицинским осмотрам, и другое). Основное требование при обработке персональных данных работника — соблюдение конституционных норм, гарантирующих охрану прав и свобод человека и гражданина.

В Европейском Союзе вопросам защиты интересов владельцев персональных данных, которые были подвергнуты электронной обработке, посвящена Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», подписанная в Страсбурге (Франция) в 1981 году. Федеральный закон о ратификации Конвенции был подписан Президентом РФ 19 декабря 2005 года Федеральным законом РФ от 19.12.2005 № 160-ФЗ

Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) (рус., англ.) (от 28.01.1981 с изменениями, внесенными Международным договором от 15.06.1999). Ратифицирована Федеральным законом РФ от 19.12.2005 № 160-ФЗ.

Под обработкой персональных данных Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» от 28 января 1981 г. понимает накопление данных, проведение логических и (или) арифметических операций с такими данными, их изменение, стирание, восстановление или распространение.

Ст.2 Определения.Для целей настоящей Конвенции:

а) «персональные данные» означают информацию, касающуюся конкретного илимогущего быть идентифицированным лица («субъекта данных»);

b) «автоматизированная база данных» означает любой набор данных, к которымприменяется автоматическая обработка;

с) «автоматическая обработка» включает следующие операции, если они полностью иличастично осуществляются с применением автоматизированных средств: накоплениеданных, проведение логических или/и арифметических операций с такими данными, ихизменение, стирание, восстановление или распространение;)

«Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» (Федеральный Закон «О персональных данных» от 27.07.2006 № 152-ФЗ).

Обработка указанных специальных категорий персональных данных допускается в случаях, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

3.Что значит, дать согласие на обработку персональных данных?

**Слайд 22**

Статья 5 Закона от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает шесть принципов обработки персональных данных, защищающих персональную информацию человека; данные принципы схожи с принципами, содержащимися во многих европейских правовых актах. Во-первых, персональные данные должны собираться и использоваться законно и добросовестно. Эта норма говорит о том, что персональные данные должны быть собраны и использованы в соответствии с законодательством РФ и только с согласия субъекта персональных данных, но за исключением случаев, четко оговоренных в части 2 статьи 6 Закона, когда такое согласие не требуется.

В соответствии с гл. 2. ст. 9 Согласие субъекта персональных данных на обработку его персональных данных.Федерального Закона «О персональных данных» от 27.07.2006 № 152-ФЗ, каждая школа разрабатывает локальный акт, который конкретизирует сведения, относящиеся к персональным данным, кто имеет доступ к персональным данным обучающегося, права и обязанности работников, получивших доступ к персональным данным ученика и утверждает форму Согласия родителя(законного представителя) на обработку персональных данных.Согласие на обработку своих персональных данных субъект персональных данных должен дать в письменной форме; содержание этого документа четко установлено в п. 4 статьи 9 Закона.К примеру, в письменном согласии субъекта должна быть обязательно указана цель обработки персональных данных и их перечень, а также срок, в течение которого действует согласие и порядок его отзыва.

гл. 2. ст. 9. ч.4.Согласие субъекта персональных данных на обработку его персональных данных

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

 В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

1. Ответственность

**Слайд 23**

Лицам, нарушившим требования Федерального Закона «О персональных данных» от 27.07.2006 № 152-ФЗ, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная (таблица 1). При этом административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб.

Наказание за разглашение персональных данных

Наказание по ст. 137 УК РФ варьируется от штрафа до лишения свободы. Совершение ничем не отягченного преступления (ч. 1 ст. 137 УК РФ) грозит одним из следующих наказаний:

* штрафом в размере до 200 000 руб. (как вариант, в размере полуторагодовой зарплаты виновного);
* обязательными или исправительными работами на срок до 360 часов или до 1 года соответственно;
* до 4 месяцев ареста;
* до 2 лет лишения свободы.

Для лиц, допустивших разглашение конфиденциальных сведений о личности в связи со своим служебным положением, наказание будет строже:

минимальный размер штрафа в этом случае составит 100 000 руб., максимальный — 300 000 руб.;

обязательные работы в ч. 2 ст. 137 не предусмотрены, а срок принудительных увеличен до 4 лет;

продолжительность ареста продлена до 5 месяцев, срока лишения свободы — до 5 лет.

Самые суровые последствия ждут виновных в разглашении данных о несовершеннолетних:

согласно ч. 3 ст. 137 УК РФ им придется заплатить от 150 000 до 350 000 руб. штрафа либо принудительно отработать до 6 лет;

в качестве альтернативы возможен арест на срок до полугода или до 6 лет тюрьмы.

Ст. 137 УК РФ — одна из наиболее сложных норм с точки зрения квалификации преступления. Для ее правильного толкования необходимо учитывать требования смежных отраслей законодательства. В частности, не избежать обращения к законам, регламентирующим обращение с персональными данными, регулирующим деятельность различных ведомств и раскрывающим понятие тайны.

**Гражданский кодекс РФ, Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации».**

**Ответственность за распространение недостоверных, но не порочащих сведений**

Ранее распространение недостоверных, но не порочащих честь, достоинство и деловую репутацию сведений не считалось нарушением. Новая норма п. 10 ст. 152 Гражданского кодекса РФ позволяет требовать:

- прекращение распространения любых не соответствующих действительности сведений,

- опровержения сведений,

· опубликования своего ответа,

· компенсации убытков и морального вреда.

В норме устанавливается специальный срок исковой давности в один год на случай распространения недостоверной информации в СМИ.

Напомним, что, если недостоверные сведения порочат честь, достоинство и деловую репутацию, именно ответчик (распространитель) должен доказать их соответствие действительности (п. 1 ст. 152 Гражданского кодекса). В случае оспаривания недостоверных сведений, которые не порочат, бремя доказывания перенесено на истца. Именно истец должен доказать, что распространенные сведения не соответствуют действительности.

**Слайд 24**

Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 29.07.2018) "О защите детей от информации, причиняющей вред их здоровью и развитию"

Закон издан на 29 страницах, состоит из 7-ми глав и 23 статей. Суть закона в следующем: все дети поделены на четыре "информационно-возрастные" категории:

* до шести лет,
* от шести до двенадцати,
* от двенадцати до шестнадцати и
* достигшие шестнадцати лет.

Для каждой - закон определяет, какую информацию можно ей предоставлять, а какую - запрещается. Федеральный закон направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию(Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Итак, какую же информацию считают «вредной» и «травмирующей».

Статья 5. Виды информации, причиняющей вред здоровью и (или) развитию детей

1. К информации, причиняющей вред здоровью и (или) развитию детей, относится:

1) информация, предусмотренная частью 2 настоящей статьи и запрещенная для распространения среди детей;

2) информация, которая предусмотрена частью 3 настоящей статьи с учетом положений статей 7 - 10 настоящего Федерального закона и распространение которой среди детей определенных возрастных категорий ограничено.

**Слайд 25**

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

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

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

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

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

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

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

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

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

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

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

В Федеральном законе от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию, введено понятие информационной безопасности детей, рассмотрены виды информации, причиняющей вред здоровью и (или) развитию детей». Федеральный закон, посвященный защите детей от вредной информации и даются принципы организации защиты детей.

**Слайд 26**

Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

Зачем принята стратегия

«Стратегия развития информационного общества» — политический документ, определяющий цели, задачи и меры по реализации внутренней и внешней политики РФ в сфере применения ИКТ».

Президент в своём указе, утверждающем «Стратегию развития информационного общества», говорит, что «Стратегия» нужна как условие формирования в стране «общества знаний». Определение последнего понятия таково: «общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учётом стратегических национальных приоритетов РФ».

«Стратегия» в нынешней редакции посвящена главным образом технологиям, информационным и телекоммуникационным как важнейшему элементу национальной инфраструктуры. Построение общества знаний и создание в России цифровой экономики в документе неоднократно упоминаются — как цель развития информационного общества.

Цель формирования информационного пространства знаний, записано в «Стратегии», состоит в «обеспечении прав граждан на объективную, достоверную, безопасную информацию и создании условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора». Отдельно говорится, в частности, об информационной безопасности детей, о «продвижении» русского языка в мире и о поддержке «традиционных», т.е. существовавших задолго до Интернета, «форм распространения знаний».

«Стратегия» прежде всего обращает внимание на безопасность информационной и телекоммуникационной инфраструктуры страны, т.е. «недопущение подмены, искажения, блокирования, удаления, снятия с каналов связи и иных манипуляций с информацией».

 Для устойчивого функционирования информационной инфраструктуры предлагается, в частности, обеспечить централизованное управление ею, постепенно перевести на госорганы и ОМСУ на использование инфраструктуры электронного правительства (её также предусматривается использовать для предоставления гражданам иных, негосударственных сервисов).

**Слайд 27**

**Персональные данные и их защита в сети Интернет**

*Жадько Н.П., руководитель методического объединения учителей информатики Курчатовского района, учитель информатики МБОУ «СОШ№45 г.Челябинска»*

Одно из неотъемлемых прав каждого интернет-пользователя — право на защиту персональных данных.

 По данным ряда опросов, больше половины россиян не знают о своих правах в Интернете. Нет среди пользователей и точного понимания того, что такое «персональные данные».

Так, в нашей стране в течение 2015 г. Роскомнадзором зарегистрировано приблизительно 33 тыс. обращений от граждан с жалобами на нарушения, связанные с публикацией их личных данных в интернете.

С развитием Интернета вопросы защиты персональных данных попали в число самых актуальных вопросов безопасности не только взрослых, но и детей.

Именно поэтому важно привлечь внимание обучающихся к проблемам и последствиям ненадлежащей обработки персональных данных и широкого распространения личной информации в информационной среде.

Одним из ключевых направлений работы по защите прав субъектов персональных данных становится информационно - просветительская деятельность, в рамках которой особое внимание уделяется несовершеннолетним пользователям интернета как одной из наиболее уязвимых категорий пользователей. Главная задача — донести до российских учителей и их учеников необходимость защиты личной информации и объяснить правила безопасного управления персональными данными в Интернете.

 **Слайд 28**

В целях осуществления профилактических мер, направленных на популяризацию правил защиты персональных данных несовершеннолетних лиц Роскомнадзор в 2014 г. провел первый Всероссийский День защиты персональных данных детей, а также

**Слайд 29**, разработал информационно-развлекательный портал для педагогов, родителей и детей  [http://персональныеданные.дети/](http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/)

 направленный на изучение вопросов, связанных с защитой персональных данных при использовании цифровых технологий.

На сайте размещены информационные материалы для детей, которые могут быть использованы как в рамках школьных уроков по теме персональных данных, так и просто в виде интересной и познавательной информации. Все материалы разрабатывались с учетом ошибок детей в онлайн среде.

Что такое персональные данные?

 **Слайд 30**

Персональные данные — это любая информация, которая имеет отношение к конкретному человеку.

Персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

Идентифицирующие данные:

фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Получается, что персональные данные — это не просто ваши фамилия или имя, персональные данные — это набор данных, их совокупность, которые позволяют идентифицировать вас, понять, что вы — это вы.

 **Слайд 31**

Виды персональных данных:

• Регистрационные идентификационные данные (паспортные данные, пароли, пин-коды, СНИЛС, индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты).

• Физические характеристики (внешние данные, биометрические данные, состояние здоровья и др.).

• Пространственная локализация (фиксация местоположения и перемещения).

• Материально-экономическое положение (движимое, недвижимое имущество, зарплата, накопления и др.).

• Официальные статусы (семейное положение, достижения, награды, наличие судимостей и т.д.).

• Профессиональная занятость (включая образование).

• Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам).

• Образ жизни и поведенческие установки (мировоззрение, ценности, интересы и хобби, социальные привычки и действия, настроения, вкусы, особенности).

• Психологические особенности (черты характера, способности, знания, умения, навыки, личностные черты).

• Хроника личных событий (личный блог, сайт и т.д.).

 **Слайд 32**

Основные понятия в рамках безопасного обращения с персональными данными в сети Интернет :

Акка́унт, учетная запись (англ. account) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Кибербу́ллинг(англ. сyberbulling) – намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

Конфиденциа́льность(англ. сonfidence – «доверие») –

1. Необходимость предотвращения утечки (разглашения) какой-либо информации.

2. Обязательное для выполнения лицом, получившим доступ к определенным сведениям (сообщениям, данным) требование не передавать их третьим лицам без согласия лица, самостоятельно создавшего информацию либо получившего право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Фи́шинг (англ. phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, социальных сетей.

Вывод очень простой — чем больше мы выкладываем о себе, тем больше о нас информации узнают другие пользователи.

Стоит отметить, что о некоторых видах данных мы не задумываемся, когда выкладываем их в сеть Интернета. Утечка важной и значимой информации может негативно отразиться на нашей жизни, поэтому необходимо обратить внимание на то, что вы размещаете.

 **Слайд 33**

МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Существуют «Три кита» защиты персональных данных:

• Надежный пароль. Надежные пароли позволят защитить от третьих лиц ваши аккаунты на онлайн-ресурсах и в приложениях.

• Управление уровнями доступа к персональным данным (настройки приватности). Настройки приватности дадут вам возможность определить уровень доступа других пользователей к вашим персональным данным, размещенным на различных онлайн-ресурсах.

 • Сознательное отношение к информации, размещаемой в интернете. Правила управления персональными данными помогут вам понять, как персональные данные, размещенные в интернете, влияют на вашу репутацию в сети.

 **Слайд 34**

Правила защиты персональных данных в Сети

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.
4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.
5. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
6. Старайтесь периодически менять пароли.
7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками. Существует несколько простых способов убедиться в подлинности ресурса:

• Всегда обращайте внимание на адресную строку браузера. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить.

• Не стоит переходить на ресурсы по ссылкам, которые вы получили по электронной почте или в личной переписке и которые требуют ввода персональных данных — многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше — используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

 • Прежде чем вводить персональные данные в интернете, убедитесь, что ресурс, на котором вы находитесь, использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры https:// вместо привычной http://, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.

• Комплексные антивирусные программы также могут помочь защититься от мошенников

 **Слайд 35**

Защита персональных данных на своем устройстве

 • Для удаления «цифровых следов» с компьютера после работы в интернете очистите журнал посещений (в браузере) и историю поисковых запросов.

• В настройках программ сетевой защиты также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами.

• Будьте внимательны с настройками мобильных приложений: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т.д., если хотите избежать случайного попадания персональных данных в сеть.

**Слайд 36**

Защита персональных данных на чужом устройстве

• При входе в свой аккаунт с чужого устройства всегда выбирайте опцию «чужой компьютер», «не сохранять пароль», «безопасный ввод» и т.д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

• Чтобы не оставить цифровых следов на чужом устройстве, используйте режим инкогнито (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

 **Слайд 37**

Защита персональных данных от третьих лиц

• Используя вкладку «настройки приватности» (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в «черный список» автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

 • Если другой пользователь использует ваши персональные данные, например фотографии, без вашего согласия, вы можете пожаловаться в службу поддержки ресурса (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

 Заключение

С развитием Интернета, уже в недалеком будущем частная жизнь станет прозрачной и публичной «по умолчанию» –персональную информацию будет невозможно не открыть государству и различным организациям, а справляться с вопросами ее безопасности будет все сложнее.

**Слайд 38, 39**

 Роскомнадзором разработаны материалы для проведения обучающих мероприятий с детьми и подростками по безопасному поведению в Интернете для двух возрастных групп детей 9-11 лет и 12-14 лет и могут быть использованы дистанционно в рамках классных часов и обучающих мероприятий со школьниками (https://pd.rkn.gov.ru/multimedia/video114.htm)

**Раздел 2. Практикум**

 **Слайд 40**

Работа по секциям

**Раздел 3. Рефлексия**

Список литературы

1. Баева И.А. Психологическая безопасность образовательной среды: учеб. пособие / под ред. И. А. Баевой. М., 2009.
2. Богатырева Юлия Игоревна, канд. пед. наук, доц., bogatirevadj@yandex.ru, Россия, Тула, ТГПУ им. Л.Н. Толстого.
3. Бочаров М.И. Комплексное обеспечение информационной безопасности школьников. // Применение новых информационных технологий в образовании. 2009.
4. Ильченко О.А. Организационно-педагогические условия разработки и применения сетевых курсов в учебном процессе (на примере подготовки специалистов с высшим образованием): автореф. дисс. канд. пед. наук. М.: Центр креативной педагогики Московской государственной технологической академии. 2002.
5. Коротенков Ю.Г. Информационная образовательная среда основной школы М.: Академия АйТи, 2011.
6. Национальная стратегия действий в интересах детей на 2012 - 2017 годы [Электронный ресурс] URL:http://www.soprotivlenie.org (дата обращения: 31.07.2013).
7. Федеральный государственный образовательный стандарт основного общего образования. М.: Просвещение, 2011.
8. [**https://rkn.gov.ru**](https://pd.rkn.gov.ru/multimedia/video114.htm)
9. [**https://pd.rkn.gov.ru/multimedia/video114.htm**](https://pd.rkn.gov.ru/multimedia/video114.htm)
10. [**http://персональныеданные.дети**](http://персональныеданные.дети/)

Перечень законодательных актов по теме

1. Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948).
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).
3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) (рус., англ.) (от 28.01.1981 с изменениями, внесенными Международным договором от 15.06.1999). Ратифицирована Федеральным законом РФ от 19.12.2005 № 160-ФЗ.
4. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию».
5. Федеральный закон от 28.07.2012 № 139-ФЗ (ред. от 14.10.2014) «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации».
6. Федеральный закон от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”».
7. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных.
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).
9. Гражданский кодекс РФ, Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации».
10. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015).
11. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

Разъяснения Роскомнадзора от 30 августа 2013 г. "Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки"