Нормативное регулирование информационной безопасности обучающихся

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации.

К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты:

1. Конституция Российской Федерации содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др.

   Например, к таким положениям относятся нормы, которые устанавливают право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п.4.ст. 29).

   Это конституционное право, устанавливающее возможность удовлетворения интересов личности и общества сбалансировано необходимостью их ограничения федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (п.3.ст.55).

   Конституция Российской Федерации устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи (ст.23).
2. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

   Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.
3. Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности. Они определяют основные термины и их определения, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст.3), классификацию информации по категориям доступа - общедоступную и ограниченного доступа (ст. 5), порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще). Закон определяет базовые положения правового режима доступа к информации (ст.8) и его ограничения (ст.9), основные параметры правовых режимов распространения (ст.10) и документирования (ст.11) информации, информационных систем (ст.13), информационно-телекоммуникационных сетей (ст.15) и общие условия защиты информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также в общих чертах описывает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
4. Федеральный закон от 21 июня 1993 № 5485-1 «О государственной тайне», Федеральные законы от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» и от

27.07.2006 г. № 152-ФЗ «О персональных данных» устанавливают правовые режимы информации ограниченного доступа, в том числе, сведений, составляющих государственную и коммерческую тайну.

5. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Нормы названного закона определяют правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства. В ст. 1 этого закона определена его цель - обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В законе сформулированы функции электронной цифровой подписи: удостоверяющая, защитная и устанавливающая.
6. Уголовный кодекс РФ в главе 28 Кодекса предусматривает ответственность за совершение преступлений в сфере компьютерной информации (ст.272-275). Всего в тексте Кодекса содержится более 50 отдельных статей, устанавливающих уголовную ответственность за нарушение установленных запретов в информационной сфере.
7. Трудовой кодекс РФ устанавливает правовой режим персональных данных работника, определяет общие требования по их обработке и защите, устанавливает сроки хранения таких данных и процедуру их использования. В случаях нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, виновные лица привлекаются к дисциплинарной, материальной, административной, гражданско-правовой и уголовной ответственности. Трудовой кодекс РФ определяет норму об ответственности за разглашение отдельных видов тайн и персональных данных.
8. Часть норм, касающихся информационных отношений, содержатся в Гражданском кодексе РФ (ГК РФ). Так, ст. 150 относит личную и семейную тайну к нематериальным благам, ст. 726 устанавливает обязанность подрядчика передать информацию заказчику, ст. 857 посвящается банковской тайне, ст. 946 – тайне страхования. Четвертая часть ГК РФ направлена на регулирование отношений в области охраны прав на результаты интеллектуальной деятельности.
9. КоАП РФ в главе 13 определяет административную ответственность за правонарушения в области связи и информации посвящена отдельная глава (ст. 13.1-13.24). В него включены еще более 90 статей, в которых определяется ответственность за совершение проступков информационного характера. Так, например, устанавливается ответственность за отказ в предоставлении гражданину информации (ст. 5.39), за сокрытие или искажение экологической информации (ст. 8.5), за незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53).

Помимо названных выше существует множество законов, непосредственно не направленных на регулирование информационных отношений, но содержащих отдельные статьи, посвященные информации или связанные с ней. К числу следует отнести следующие федеральные законы: от 13.03.2006 № 38 -ФЗ «О рекламе»; от 29.12.1994 № 78-ФЗ «О библиотечном деле»; от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»; от 17.07.1999 № 176-ФЗ «О почтовой связи»; от 17.08.1995 № 147-ФЗ «О естественных монополиях»; от 21.02.1992 № 2395-1 «О недрах».

Имеется также массив нормативных правовых актов подзаконного характера, состоящий из большого количества документов, регулирующих отдельные направления правового обеспечения информационной безопасности.

а) указы Президента:

– от 11.02.2006 № 90 «О перечне сведений, отнесенных к государственной тайне»;

– от 06.10.2004 № 1286 «Вопросы межведомственной комиссии по защите государственной тайны»;
– от 17.05.2004 № 611 «О мерах по обеспечению безопасности РФ в сфере международного информационного обмена»;
- от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». В данном Указе устанавливается запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну к информационно-телекоммуникационным сетям международного информационного обмена. В целях защиты информации государственные органы обязаны использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данных требований Указа в полной мере должно обеспечить защиту информации, составляющей государственную тайну.
– от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
– от 15.01.2913 № 31/с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».
б) постановления Правительства:
– от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти»;
– от 27.05.2002 № 348 «Об утверждении Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»; – от 18.02.2005 № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий»;
– от 22.08.1908 № 1003 «О порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне»;
– от 28.10.1995 № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне»;
– от 26.10.2012 № 1101 «О создании единой автоматизированной системе «Единый реестр доменных имен, указателей страниц, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в РФ запрещено».

Наряду с указами Президента РФ и постановлениями Правительства источниками информационного права выступают акты центральных органов государственного управления РФ (ведомственные нормативно-правовые акты). В области информационных отношений существует значительное их количество. Тематика и направленность данных актов зависит от компетенции издавшего их органа.

Так, приказом Федеральной службы безопасности (ФСБ) РФ от 13.11.1999 № 564 утверждено «Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну», которое определяет организационную структуру системы сертификации, порядок проведения сертификации и инспекционного контроля, требования к нормативным и методическим документам по сертификации, а также виды средств защиты информации, подлежащих сертификации.
Приказом ФСБ РФ от 09.02.2005 № 66 утверждено «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации)».

Важный элемент системы законодательства РФ в информационной сфере – международные соглашения. В соответствии с ч. 4 ст. 15 Конституции РФ нормы международных договоров обладают приоритетом по отношению к противоречащим им правилам внутригосударственных законов. Это относится как к многосторонним, так и к двусторонним договорам.

Особое место среди многочисленных многосторонних соглашений, содержащих информационные нормы, занимают:

– «Всеобщая декларация прав человек» от 10.12.1948;

– «Международный пакт о гражданских и политических правах» от 10.12.1966;

– «Заключительный акт совещания по безопасности и сотрудничеству в Европе» от 01.08.1975.

В этих документах нашли свое воплощение международные принципы и стандарты, провозглашающие право на свободу информации, которые, однако, налагают особые обязанности и особую ответственность, сопряженные с некоторыми ограничениями прав и свобод.

Важнейший документ, посвященный организации и активизации деятельности международного сообщества в области формирования глобального информационного общества, – «Окинавская хартия глобального информационного общества», принятая в июле 2000 г. представителями восьми ведущих стран. Этот документ устанавливает основные принципы вхождения государств в глобальное информационное общество.

Приказом ФСО России от 07.08.2009 N 487 утвержденоПоложение о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Эксплуатацию, поддержание и развитие сегмента информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации обеспечивает Служба специальной связи и информации ФСО России.

В соответствии с названным нормативным правовым актом Сегмент сети Интернет – это находящаяся в ведении (эксплуатации) Федеральной службы охраны Российской Федерации (далее именуется - оператор сегмента сети Интернет) часть информационно-телекоммуникационной сети, связывающей информационные системы, информационно-телекоммуникационные сети различных государств посредством сетевых адресов информационно-телекоммуникационной сети Интернет (далее именуется - сеть Интернет).

Сегмент сети Интернет предназначен для обеспечения размещения информации о деятельности Администрации Президента Российской Федерации, Аппарата Совета Федерации Федерального Собрания Российской Федерации, Аппарата Государственной Думы Федерального Собрания Российской Федерации, Аппарата Правительства Российской Федерации, аппаратов Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации, Генеральной прокуратуры Российской Федерации и Следственного комитета при прокуратуре Российской Федерации, федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, а также для доступа к сети Интернет должностных лиц указанных государственных органов (далее именуются - пользователи сегмента сети Интернет).

Функционирование сегмента сети Интернет обеспечивается путем применения стандартных протоколов сети Интернет и регламентов обмена информацией в порядке, определяемом оператором сегмента сети Интернет.

В российском правовом пространстве длительное время в обороте используется «служебная информация ограниченного распространения» о деятельности органов

государственной власти, которая нередко упоминается в нормативных правовых актах как «служебная тайна».

Постановление Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти» определяется правовое положение информации ограниченного доступа, несмотря на то, что п.п.1 и 4 ст.9 ФЗ «Об информации» ограничение доступа к информации и, в частности, отнесение информации к сведениям, составляющим служебную тайну, устанавливаются исключительно федеральными законами. Явное несовершенство информационного законодательства и практики его применения отрицательно влияет на состояние правовой защиты интересов субъектов правоотношений. Пробел в нормативных правовых актах, устанавливающих оборот информации служебного характера, не позволяет установить запрет либо ограничения на ее использование, а вместе с этим создает ситуацию невозможности установить административную и / или уголовную ответственность за нарушения порядка распространения этой важной формы информации.

Тема информационной безопасности образовательной организации актуальна в настоящее время, т. к. работа в том числе учащихся в сети Интернет стала неотъемлемой частью учебного процесса. Несмотря на то, что Интернет — это, в первую очередь, информационная сеть, содержащая колоссальное количество познавательных и развивающих сайтов, посещение которых способствует быстрому поиску информации для домашнего задания/доклада/самостоятельной работы, зачастую подросток пользуется просторами Интернета для личных целей. В российском законодательстве существует ряд нормативно — правовых документов, регулирующих вопросы информационной безопасности, а также подписанные международные акты. Одним из основополагающих международных актов, ратифицированных в том числе Российской Федерацией, является Окинавская хартия. С момента ее подписания Россия стала активным членом глобального информационного общества, принимая участие в процессе его формирования не только на национальном, но и на международном уровне. Основными принципами построения информационного общества, согласно хартии, определены укрепление доверия и безопасности при использовании информационно — телекоммуникационных технологий и верховенство права. В Российском законодательстве основным документом, определяющим право на личную информационную безопасность, является Конституция Российской Федерации, где в ст. 23 прописано, что каждый гражданин имеет право на личную тайну и тайну переписки [1]. В последние годы активизировался вопрос реализации задач, связанных с информационной безопасностью и борьбой с кибертерроризмом. В первую очередь это проявилось в принятии в 2006 году федерального закона «Об информации, информационных технологиях и о защите информации», в котором были сформулированы положения об информации как объекте правового регулирования, а также в подписании в феврале 2008 года Концепции «электронного правительства» и Стратегии развития информационного общества в Российской Федерации, которая является базовым документом по планированию развития системы обеспечения национальной, в том числе и информационной безопасности в России, в которой излагаются порядок действий и меры по обеспечению национальной безопасности.

В сентябре 2000 года Президентом РФ была подписана Доктрина информационной безопасности Российской Федерации, которая стала одним из первых документов, определяющих вопросы информационной безопасности. Доктрина представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства [4]. Для обеспечения надежной защиты персональных данных был принят Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Говоря непосредственно об

образовании, стоит отметить, что в каждом образовательном учреждении создана и успешно функционирует информационно — образовательная среда. Ее значение в последнее время возрастает, она качественно влияет на образовательный процесс, все субъекты образования и на их отношения в образовательной системе. В качестве предмета информационной открытости выступает сайт образовательной организации, который, как правило, содержит всю необходимую информацию об учреждении, а также новости и дополнительную информацию (мероприятия, памятки для учащихся и родителей и др.). Являясь неотъемлемым элементом структуры государственной власти, система образования также обеспечивает открытость своих данных. Необходимость открытости данных образовательных организаций закреплена в ст. 29 Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»: «Образовательные организации формируют открытые и общедоступные информационные ресурсы, содержащие информацию об их деятельности, и обеспечивают доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети «Интернет»». Информационная безопасность в образовании обеспечивается на основе Национальной стратегии действий в интересах детей на 2012–2017 гг., где обозначен порядок создания порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей, регулируются вопросы стимулирования родителей к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа детей в сети Интернет. Основополагающим документом в вопросе информационной безопасности детей в образовательной организации является Федеральный Закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», содержащий в себе основные ограничения и требования к информационной продукции, которая может находится в доступном для детей варианте. Информационная сфера так многогранна, что правовое обеспечение информационной безопасности при построении информационного общества, которое позволяло бы защитить интересы личности, общества и государства, приобретает первостепенное значение.

Подготовлено на основании Методических рекомендаций Министерства образования и науки российской федерации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (Письмо от 14 мая 2018 г. N 08-1184).