

ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВОВОЙ ЗАЩИТЫ

*Заузолкова Ю. П., преподаватель общеобразовательных дисциплин
ГАПОУ СО «Нижнетагильский горно-металлургический
колледж им. Е. А. и М. Е. Черепановых»*

В нашей жизни устойчиво закрепилось понятие «информация», которая играет особую роль в процессе развития общества. Информация может быть, как в материальном, так и в нематериальном (нефиксированном) виде, но вне зависимости от этого, согласно статьи 128 Гражданского Кодекса РФ информация определяется как объект права и требует правового регулирования.

Само понятие «Информация» раскрывает Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации») как сведения (сообщения, данные) независимо от формы их представления. То есть это могут быть сведения о лицах, предметах, фактах, событиях, явлениях и процессах. Искажение информации, блокирование процесса ее получения или внедрение ложной информации влечет наступление юридических последствий.

Основными нормативными правовыми актами, регламентирующими информацию и её использование, прежде всего, являются Конституция Российской Федерации и ранее упомянутый ФЗ «Об информации».

В Конституции закреплены основные права и свободы граждан Российской Федерации. В том числе в ней введены базовые положения, касающиеся вопросов обработки и защиты информации; виды защищаемой информации (государственная тайна, коммерческая тайна, персональные данные и т.п.).

Статья 23 Конституции РФ устанавливает, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну. В статье 24 устанавливается, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. А в части 4 статьи 29, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

ФЗ «Об информации» вводит определения основных понятий в сфере обработки и защиты информации, которые используются во всем правовом поле Российской Федерации, а также регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. Правовое регулирование отношений, связанных с защитой информации основывается на таких принципах, как:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 4) достоверность информации и своевременность ее предоставления;
- 5) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

В рассматриваемом вопросе основным, безусловно, является информация. Закон не требует, чтобы сведения были каким-либо образом структурированы, были зафиксированы на каком-либо носителе и т. п. Статья 5 ФЗ «Об информации» устанавливает, что информация может являться объектом публичных, гражданских и иных правовых отношений и может свободно использоваться, и передаваться одним лицом другому, если федеральными законами

не установлены ограничения доступа к ней, либо требования к порядку ее предоставления или распространения.

В зависимости от категории доступа к ней информация подразделяется на общедоступную и информацию, доступ к которой ограничен федеральными законами. А в зависимости от порядка предоставления или распространения информация подразделяется на:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

При работе с информацией мы предъявляем к ней определенные требования: например, к форме ее представления, объему данных, новизне и т.д.

Обладателем информации может быть гражданин, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование (ст. 6 ФЗ «Об информации»).

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
- 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
- 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

При осуществлении своих прав обладатель информации обязан:

- 1) соблюдать права и законные интересы иных лиц;
- 2) принимать меры по защите информации;
- 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Комплекс мер, необходимых для защиты информации от утечки или взлома, или информационная безопасность, содержит три основных свойства безопасности информации: конфиденциальность, целостность и доступность.

Конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (п. 7 ст. «ФЗ «Об информации»»). То есть это некоторое ограничение, наложенное на информацию ее владельцем. Каждый, кто желает получить такую информацию, должен согласиться с тем условием, что он не может своим собственным решением передать такую (конфиденциальную) информацию третьим лицам, а должен предварительно получить согласие обладателя на передачу или обеспечить получение третьей стороной информации непосредственно у обладателя.

Целостность информации - означает, что цифровая информация не повреждена и может быть доступна или изменена только теми, у кого есть права на такие изменения. Целостность включает в себя поддержание согласованности, точности и достоверности данных на протяжении всего их жизненного цикла. Например, в рабочем чате размещаем документ и выставляем запрет

на «совместное редактирование. Если же этого не сделать, то документ будет доступен всем участникам чата и любой может внести какие-то изменения и поправки, либо вовсе безвозвратно удалить файл.

Доступность информации - состояние информации, когда лицу, обладающему правом доступа к информации и выполнившему все необходимые условия для получения этого доступа, не может быть отказано в нем. То есть доступность информации гарантируется только лицу, которое имеет право на получение данной информации. Если Вы обладаете правом на получение информации, одного желания ее получить недостаточно. Требуется также соблюдение всех необходимых условий. Например, для получения информации о банковском счете мы должны не просто обратиться в онлайн-банк, но и предъявить определенную информацию, идентифицирующую нас (логин, пароль и/или одноразовый код, приходящий на определенное устройство). Или для закрытия нашего счета в банке необходимо не только прийти в банк, но и подтвердить нашу личность, предъявив паспорт и, возможно, другие документы.

Доступ может быть получен не ко всякой информации. Например, мы можем получить доступ к состоянию своего банковского счета, но не можем получить доступ к банковскому счету стороннего лица.

В соответствии со статьей 5 ФЗ «Об информации» информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации, либо иные требования к порядку ее предоставления или распространения.

В зависимости от категории доступа к информации она подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В зависимости от порядка предоставления или распространения информация подразделяется на:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Нарушение требований федерального законодательства в сфере обработки и защиты информации может повлечь различные виды ответственности: дисциплинарную, гражданско-правовую, административную или уголовную. Внутри организаций и предприятий может предусматриваться дисциплинарная ответственность (замечание, выговор или увольнение). Так подпункт «в» пункта 6 статьи 81 Трудового Кодекса РФ предусматривает основание для увольнения работника по инициативе работодателя по причине разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

Согласно п. 2 ст. 17 Федерального закона "Об информации, информационных технологиях и о защите информации" лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием

такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. При этом требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования защиты информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

В ст. 1100 и 1101 ГК РФ определено, в частности, что компенсация морального вреда осуществляется в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию. Компенсация морального вреда осуществляется в денежной форме и независимо от вины причинителя вреда.

Гражданско-правовая ответственность за правонарушения в информационной сфере подразделяется на договорную и внедоговорную. Договорная ответственность возникает при нарушении условий договора, которым предусмотрены санкции, прямо не обеспеченные нормами действующего законодательства. Внедоговорная ответственность возникает при причинении личности потерпевшего или его имуществу вреда, который не связан с неисполнением нарушителем договорных обязательств.

Серьезные проступки могут оказаться составом административного правонарушения или даже уголовного преступления. В соответствии с частью 2 статьи 13.12 Кодекса Российской Федерации об административных правонарушениях использование несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

В соответствии со статьей 137 Уголовного кодекса Российской Федерации незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

В соответствии со статьей 272 Уголовного кодекса Российской Федерации неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Защите информации от неправомерного овладения ею отводится весьма значительное место. При этом целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Список используемых источников:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_28399/?ysclid=m8mw3lqgcm76227375
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=m8mw69ebpj118525491
3. Гражданский кодекс Российской Федерации часть 1 (ГК РФ) от 30 ноября 1994 года N 51-ФЗ (последняя редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_5142/
4. Гражданский кодекс Российской Федерации часть 2 (ГК РФ) от 26 января 1996 года N 14-ФЗ (последняя редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_9027/
5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 03.02.2025) (с изм. и доп., вступ. в силу с 01.03.2025). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m8mx9zaalx429792857
6. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 28.12.2024) https://www.consultant.ru/document/cons_doc_LAW_34683/?ysclid=m8mxcftg53440699110
7. Вострецова, Е.В. В78 Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с. Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf