Федеральное государственное бюджетное образовательное учреждение
дополнительного профессионального образования
«Приволжский институт повышения квалификации
Федеральной налоговой службы»,
г. Нижний Новгород

Профессиональная переподготовка по программе
«Информационная безопасность»

КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: Правонарушения в сфере защиты конфиденциальной информации, особенности их выявления в рамках служебных полномочий

Автор работы:
слушатель группы ЗИБ

Руководитель:

Нижний Новгород
2022

СОДЕРЖАНИЕ

Введение……...3
1. Особенности правового регулирования конфиденциальной информации……..6
1.1. Понятие конфиденциальной информации…….6
1.2. Виды конфиденциальной информации……11
1.3. Основные источники правового регулирования конфиденциальной информации……....15
2. Актуальные вопросы противодействия совершению правонарушений в сфере защиты конфиденциальной информации…….……..……...21
2.1. Общая характеристика и виды правонарушений в сфере защиты конфиденциальной информации……..21
2.2. Механизмы выявления правонарушений в сфере защиты конфиденциальной информации в рамках служебных полномочий……...25
2.3. Особенности защиты конфиденциальной информации ФНС России. Проблемы и пути совершенствования системы защиты конфиденциальной информации……32
Заключение……40
Библиография……43

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена теоретической и практической значимостью вопросов, связанных с информационно-правовым регулированием порядка выявления правонарушений в сфере защиты конфиденциальной информации.

Информация - важнейший продукт общественного производства, постоянно наращиваемый ресурс человечества; сегодня это наиболее ценный и ходовой объект в международных экономических отношениях. На международном уровне сформировалась система взглядов на информацию как на ценнейший ресурс жизнеобеспечения общества, имеющий социальное значение.

Вся информация представляет различную ценность для субъекта и, соответственно, ее разглашение может привести к угрозам экономической безопасности различной степени тяжести. Боязнь лишиться таких активов заставляет создавать различные системы защиты, в том числе и организационную, а главное - правовую. В связи, с чем информация разделяется на три группы: информация для открытого пользования любым потребителем в любой форме; информация ограниченного доступа - только для органов, имеющих соответствующие законодательно установленные права (полиция, налоговая инспекция, прокуратура); информация только для работников (либо руководителей) организации. Информация, относящаяся ко второй и третьей группам, является конфиденциальной и имеет ограничения в распространении. Часть этой информации составляет особый блок и может быть отнесена к тайне. Важным направлением в сфере законодательства по вопросам информационной безопасности является определение юридической ответственности за совершение противоправного деяния в этой области. Юридическая ответственность - это важная мера защиты интересов личности, общества и государства. Она наступает в результате нарушения предписаний правовых норм и проявляется в форме применения к правонарушителю мер государственного принуждения.

Безопасность информационной системы – это свойство, заключающее в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации. Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

В формирующемся современном мире информация выступает

важнейшим компонентом развития общества. Нынешнее гражданское общество постепенно превращается из информированного в информационное, поэтому можно смело констатировать, что XXI век по праву считается веком информации. Информация приобретает глобальный характер; не существует границ для потока информации; информация является значимой как для себя лично, так для государства и общества в целом; каждый может искать, получать, передавать, производить и распространять информацию любым законным способом. Информационное общество развивается стремительными темпами, и это развитие сказывается на характере общественных отношений, которые формируется между людьми, а также между ними и государством.

В настоящее время провозглашена программа по созданию единого информационного пространства России, формирование и развитие которого необходимо для обеспечения оперативного доступа граждан к сведениям, имеющимся в информационных системах, а также в целях реализации полномочий органов государственного управления в сфере управления экономикой, в области безопасности личности, общества и государства с преимущественным использованием информационных систем. При правовом регулировании использования информационных систем важную роль играет проблема установления порядка доступа к информации, которая функционирует в различных видах тайн.

Поэтому порядок доступа устанавливается органами государственного управления в соответствии с законом, а использование такой информации регулируется правовыми режимами оборота информации конфиденциального характера. Обеспечение конфиденциальности в процессе оборота информации является обязательным условием, определяющим дальнейшую деятельность органов государственного управления, и оборот информации конфиденциального характера в этих органах регулируется правовыми режимами служебной тайны и персональных данных. Исследование правовых режимов служебной тайны и персональных данных вынужденная мера, так как не разработанность данных режимов на современном этапе затрагивает не только граждан, но и органы государственного управления. Главенствующая цель правового режима служебной тайны и персональных данных заключается в обеспечении защиты прав субъектов, которые предоставляют информацию конфиденциального характера в органы государственного управления, а также контроль за тем, как должностные лица реализуют право на

ограничение информации, которая создается в данном органе в интересах государственного управления.

Все эти факторы в совокупности обусловили возникновение научного интереса к правовым режимам оборота информации конфиденциального характера в сфере государственного управления.

Практическая значимость даннойработы заключается вусовершенствовании методики выявления и предотвращения правонарушений в сфере защиты конфиденциальной информации в процессе работы территориальных налоговых органов;

Объект исследования: правовые и организационные особенности выявления правонарушения в сфере защиты конфиденциальной информации.

Предмет исследования: механизмы выявления правонарушений в сфере защиты конфиденциальной информации.

Цель исследования: изучитьправонарушения в сфере защиты конфиденциальной информации иопределить особенности их выявления в рамках служебных полномочий.

Для достижения поставленной цели определены следующие задачи выпускной квалификационной работы:

1) рассмотреть понятие, виды и структуру конфиденциальной информации;

2) изучить организационно-правовые механизмы выявления правонарушений в сфере защиты информации;

3) изучить нормативно-правовые основы защиты конфиденциальной информации;

4) проанализировать систему защиты конфиденциальной информации, в том числе и персональных данных;

5) обосновать предложения и рекомендации по совершенствованию системы выявления правонарушений в сфере защиты конфиденциальной информации.

ГЛАВА I. ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. 1. Понятие конфиденциальной информации

В широком смысле слова, конфиденциальная информация – это сведения с ограниченным доступом. В узком смысле, конфиденциальная информация имеет особую ценность для лиц, пребывающих на государственной службе или работающих в организации.

Законодатель раскрывает понятие «конфиденциальность информации» в Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее – Федеральный закон № 149-ФЗ). Согласно ст. 2 Федерального закона № 149-ФЗ, к данным ограниченного доступа относятся сведения, которые не могут быть переданы третьим лицам без согласия на это обладателя данных.

Конфиденциальная информация представляет собой определенную тайну, поскольку она доступна только нескольким категориям лиц, имеющим право и доступ на работу с ней. Охрана и правовая защита конфиденциальных данных гарантирована государством и закреплена в Конституции РФ. В основном законе РФ указано, что гражданин, организация и государство, имеют право на тайну.[1]

Основными источниками правового регулирования конфиденциальной информации в РФ являются:

- международные договоры и соглашения;
- конституция РФ;
- федеральные законы;
- законы субъектов;
- локальные акты.

В информационной безопасности и защите информации специалисты придерживаются следующего определения: конфиденциальность информации — свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

С развитием информационных технологийпроблема конфиденциальности и конфиденциальной информации приобретает большую значимость. И в различных областях и различных странах конфиденциальность и информация, относящаяся к конфиденциальной определяется по-разному.

В странах Европейского союза конфиденциальность информации регулируется с помощью ряда соглашений и директив, таких как директива EC 95/46/EC, 2002/58/EC и ETS 108, ETS 181, ETS 185, ETS 189.

Так, конвенция «О преступности в сфере компьютерной информации» (ETS № 185) направлена на сдерживание, в том числе, действий,

---

[1]Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореферат дис. канд. юрид. наук. - М., 2014. С. 25-27.

направленных против конфиденциальности компьютерных данных и компьютерных сетей, систем. Согласно данной конвенции для противодействия преступлениям против конфиденциальности доступности и целостности компьютерных данных и систем каждая сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно её внутригосударственному праву:

Противозаконный доступ

Неправомерный перехват

Воздействие на данные

Воздействие на функционирование системы

Противозаконное использование устройств.

Согласно конвенции «О защите физических лиц при автоматизированной обработке персональных данных» (ETS N 108) стороны должны соблюдать секретность или конфиденциальность при обработке персональных данных, а также в отношении информации сопровождающей ходатайство о помощи.

Директива «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (N 95/46/EC) затрагивает вопрос конфиденциальности в своей области. Согласно данной директиве, «оператор» — физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; когда цели и способы обработки определены законодательством или подзаконными актами на национальном уровне или уровне Сообщества, оператор или конкретные критерии его назначения могут быть установлены национальным законодательством или законодательством Сообщества. А «обработчик» — это физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который обрабатывает персональные данные от имени оператора. Для обеспечения конфиденциальности, любое лицо, действующее под руководством оператора или обработчика, включая самого обработчика, которое имеет доступ к персональным данным, не может их обрабатывать, кроме как по поручению оператора, если оно не обязано это делать по закону.

Согласно, дополнению к директиве № 95/46/EC, директива 2002/58/EC, конфиденциальность относительно обработки персональных данных и защите частной жизни в электронном коммуникационном секторе заключается в запрете просмотра, записи или хранения, а также других способах вмешательства или наблюдения за сообщениями и относящего к ним данным по трафику, осуществляемые лицами или другими пользователями без согласия самого пользователя.

На данный момент в российском законодательстве чёткого определения понятия «конфиденциальная информация» нет. В утратившем силу Федеральном законе от 20.02.1995 № 24-ФЗ "Об информации, информатизации и защите информации"говорится, что конфиденциальная

информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.[2]

Действующий Федеральный закон № 149-ФЗтермина «конфиденциальная информация» не содержит. Однако, он описывает понятие «конфиденциальности». «Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя». Согласно этому же закону «информация — сведения (сообщения, данные) независимо от формы их представления».

В Указе Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера" (далее – Указ Президента № 188) к сведениям конфиденциального характера относят:

Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная 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 или иных сообщений и так далее).

Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Таким образом, в Российской Федерации конфиденциальность определяется как обязательное для выполнения лицом, получившим доступ к определённым сведениям (сообщениям, данным) независимо от формы их представления, требование не передавать их третьим лицам, без согласия лица, самостоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Выше был приведен список сведений которые относят к конфиденциальным. Но закон «Об информации» разрешает обладателю информации наделять её статусом конфиденциальности самостоятельно. Поэтому, список в Указе Президента

---

[2] Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА. Закон и право 2017. С. 10-13.

№ 188 является примерным.

Понятие конфиденциальности используется практически во всех областях, как в коммерческих структурах, так и государственных. Когда речь заходит о конфиденциальности на предприятиях, то чаще всего имеется в виду коммерческая или государственная тайна.

Конфиденциальность — обязательство неразглашения информации, полученной от испытуемого (в общем случае, от делового партнера, от участника переговоров, собеседника), или в общем случае ограничение её распространения кругом лиц, о которых испытуемый был заранее извещен.[3]

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Коммерческая тайна — режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Информация, составляющая коммерческую тайну (секрет производства), — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Принятие решений, что относить к коммерческой тайне лежит на лице занимающимся предпринимательской деятельностью, однако есть перечень сведений, на которые подобный режим не может быть наложен:

Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

Содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

О составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке,

---

[3]Богдановская И.Ю. Право на доступ к информации. Доступ к открытой информации М.: ЗАО "Юстицинформ" 2019. С. 59-60.

безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

О задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

О нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

О перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Основные меры по охране конфиденциальности информации, принимаемые её обладателем, включают:

Определение перечня информации, составляющей коммерческую тайну;

Ограничение доступа к информации, составляющей коммерческую тайну, путём установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

Учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).[4]

---

[4]Богдановская И.Ю. Право на доступ к информации. Доступ к открытой информации М.: ЗАО "Юстицинформ" 2019. С. 26-28.

В психологии конфиденциальность — это одно из основных прав испытуемого. Информация получаемая при обследовании или эксперименте не должна быть доступной третьим лицам в том случае, если это может смутить испытуемого или причинить ему вред. Кроме того, использование полученной информации ограничивается научными целями, о чём испытуемому нужно сообщить до получения информированного согласия.

В процессе психологического исследования вопрос конфиденциальности затрагивается во время сбора данных и помещения их на хранение, а также при обнародовании результатов.

В подобных случаях конфиденциальность обеспечивается путём использования кодов вместо имен, или же если речь идет об обнародовании информации, то изменением имен и опускание географической информации.

1. 2. Виды конфиденциальной информации

Конфиденциальная информация делится на несколько видов в зависимости от содержания и от того, в каком кругу используется:

1. Служебная тайна.

Согласно Указу Президента № 188под служебной тайной понимают информацию, имеющую особую ценность, доступ к которой ограничивается государственными органами РФ в соответствии с действующим законодательством.

Информация, являющаяся служебной тайной, также регулируется положениями Постановления Правительства РФ № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

В указанном Постановлении закреплены правовые положения о работе с информацией, составляющей служебную тайну:

•обязательное проставление отметки «Для служебного пользования»;

•передача сотрудникам информации, содержащей служебную тайну, только под расписку;

•хранение сведений «Для служебного пользования» в сейфах;

•уничтожение документов, содержащих служебную тайну только по акту;

•копирование документов со служебной тайной с письменного согласия руководителя.

2.Налоговая тайна.

Налоговая тайна - это любые сведения о налогоплательщике, которые получены инспекцией и иными госорганами (п. 1 ст. 102 НК РФ). Например, о контрагентах и условиях сделок с ними, об остатках денег на счетах и депозитах, о способах налогового учета отдельных операций.

Также к налоговой тайне относится коммерческая тайна, например, секреты производства и иные производственные, технические,

экономические, организационные сведения (п. 2 ст. 102 НК РФ).

Налоговая тайна не подлежит разглашению. Однако налоговый орган в некоторых случаях обязан передавать сведения, составляющие налоговую тайну (п. 2 ст. 102 НК РФ). Например, по запросу полиции или судей (пп. 29 ч. 1 ст. 13 Федерального закона от 07.02.2011 N 3-ФЗ "О полиции", ч. 6 ст. 1 Закона РФ от 26.06.1992 N 3132-1 "О статусе судей в Российской Федерации").

Не являются налоговой тайной, в частности, следующие сведения (п. 1 ст. 102 НК РФ):

•общедоступные сведения, например данные об организации из ЕГРЮЛ (п. 1 ст. 6 Закона о регистрации юридических лиц и ИП) или данные бухгалтерской отчетности, которые можно получить в государственном информационном ресурсе по запросу (ч. 9 ст. 18 Закона о бухгалтерском учете);

•о применяемомспецрежиме, о среднесписочной численности работников;

•о налоговых нарушениях и ответственности за них, в том числе о недоимке и задолженности по пеням и штрафам;

•о примененных инспекцией обеспечительных мерах (способах обеспечения исполнения обязанности по уплате налогов, сборов, страховых взносов);

•об уплаченных за прошлый год налогах и сборах;

•о суммах доходов и расходов по данным бухгалтерской (финансовой) отчетности за прошлый год;

•об участии в КГН;

сведения, направляемые налоговым (таможенным, правоохранительным) органам других государств по международным договорам о взаимном сотрудничестве.

3. Коммерческая тайна.

В соответствии со ст. 3 Федерального закона «О коммерческой тайне» № 98-ФЗ (далее – Федеральный закон № 98-ФЗ), под коммерческой тайной понимается режим ограничения использования, передачи и распространения информации, которая позволяет ее обладателю получить материальную или нематериальную выгоду.

Обладание чужой коммерческой тайной позволяет конкурентам увеличить прибыль, избежать лишних расходов, получить привилегии на рынке товаров и услуг.[5]

Согласно Федерального закона № 98-ФЗ, сведениями, составляющими коммерческую тайну, могут быть результаты интеллектуальной деятельности, научно-техническая информация, которая представляет собой особую коммерческую ценность для организации.

Ценность коммерческой тайны заключается в том, что она известна

---

[5] Козлов В.В. Сохранение коммерческой тайны в организации // Управление персоналом. 2019. № 7. С. 15-19.

лишь определенному кругу лиц и недоступна третьим лицам. Примером коммерческой тайны может служить производство по уникальной технологии какой-либо продукции.

Законодатель, помимо прочего, указывает, какие сведения не могут признаваться коммерческой тайной:

•сведения из единого государственного реестра юридических и физических лиц, подтверждающие факт внесения записи в реестр;

•лицензии и сертификаты, которые дают право заниматься предпринимательской деятельностью;

•сведения о количестве сотрудников и размере заработной платы на предприятии;

•информация, касающаяся задолженности или невыплаты заработной платы и любых социальных выплат;

•сведения о нарушении законов и привлечении к юридической ответственности;

•информация, касающаяся безопасности граждан, общества в целом и окружающей среды;

•список лиц, имеющих право совершать юридические действия без доверенности;

•информация о проведении конкурсов или аукционов по приватизации государственной или муниципальной недвижимости.

4. Персональные данные.

Федеральный закон «О персональных данных» № 152-ФЗ (далее – Федеральный закон № 152-ФЗ) поясняет, что можно считать персональными данными. Исходя из ст. 3 Федерального закона № 152-ФЗ, персональные данные – это любые сведение относящиеся (прямо или косвенно) к субъекту персональных данных, то есть физическому лицу.

Согласно закону, получение, обработка, хранение и иные действия с персональными данными физического лица, производятся только с согласия последнего.

При этом лицо, которое занимается обработкой персональных данных, не имеет права разглашать сведения, которые ему предоставляет гражданин. В исключительных случаях допускается передача таких данных, если физическое лицо лично дает на это согласие, либо это предусмотрено действующим законодательством.[6]

5. Тайна уголовного судопроизводства.

В Уголовно-процессуальном кодексе РФ (далее - УПК РФ), закреплено положение, которое запрещает разглашать сведения, касающиеся уголовного дела на стадии предварительного расследования.

Следователь или дознаватель обязан сообщить участникам уголовного судопроизводства о недопустимости разглашении сведений по уголовному делу, о чем составляется соответствующая расписка.

---

[6] Данилов А.Д. Ценность информации // Технологии информационного общества. 2011. № 10. С. 137-140.

Однако в ст. 161 УПК РФ говорится о том, что в исключительных случаях данные предварительного расследования могут предать гласности с разрешения лиц, ведущих расследование. Также, законодатель отмечает, что информация, которая может быть оглашена, не должна противоречить интересам следствия и участников уголовного судопроизводства.

При этом запрещается разглашение сведений, которые содержат информацию о частной жизни участников уголовного дела, а также несовершеннолетних граждан, которые не достигли возраста 14 лет.

6. Судебная тайна.

В судопроизводстве также существует конфиденциальная информация, которая называется судебная тайна. В любой отрасли права (административной, гражданской и уголовной) законодатель закрепляет принцип ее соблюдения.

Сущность данного принципа состоит в следующем:

•судья или коллегия судей выносят решение только в совещательной комнате;

•никто, кроме судей, не имеет право участвовать при вынесении решения, за исключением присяжных заседателей;

•при участии в судебном разбирательстве присяжные заседатели не имеют права разглашать решения суда;

•неразглашение информации по делам особой категории. Несмотря на то, что в РФ одним из принципов судопроизводства является гласность, то есть открытость судебного заседания, имеется ряд дел, по которым заседание в обязательном порядке должно быть закрытым. К таким делам, например, относятся все дела, касающиеся защиты прав и интересов несовершеннолетних.[7]

7. Профессиональная тайна.

Профессиональная тайна есть практически в каждой профессии: врач, адвокат, нотариус, психолог. Для каждого специалиста существует особое понятие профессиональной тайны, которая регламентированное в различных правовых актах.

Например, адвокаты руководствуются Федеральным законом № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации». В ст. 8 закона указано, что адвокатской тайной признаются сведения, которые стали известны адвокату при оказании юридической помощи своему доверителю. При этом недопустим допрос адвоката по обстоятельствам, которые стали ему известны в ходе профессиональной деятельности.

Аналогичные правовые положения закреплены для нотариусов, врачей и иных специалистов, получающих сведения, которые не подлежат разглашению. Каждый сотрудник, который получает доступ к данным, подписывает документ о неразглашении сведений.

---

[7] Лопатин, В.Н. Правовая охрана и защита права на тайну / В.Н. Лопатин // Юридический мир. 2018. №7. С.36 - 37.

1. 3. Основные источники правового регулирования конфиденциальной информации

В предыдущих разделах были упомянуты некоторые источники, регулирующие правовые режимы конфиденциальной информации. Остановимся на этой теме более подробно.

Обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

1. Нормативные правовые акты РФ.

2. Нормативно-методические и методические документы.

3. Стандарты.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

Акты федерального законодательства;

Международные договоры РФ;

Конституция РФ;

Законы федерального уровня (включая федеральные конституционные законы, кодексы);

Указы Президента РФ;

Постановления правительства РФ;

Нормативные правовые акты федеральных министерств и ведомств;

Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Приведем примеры:

Основные направления правового регулирования информационных отношений - конституционное и гражданско-правовое. Как продолжение свободы мысли и слова, которая закреплена в ч. 1 ст. 29 Конституции РФ, ч. 4 ст. 29 Конституции РФ закрепляет право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется соответствующим федеральным законом. Этому праву корреспондирует общая обязанность органов государственной власти и местного самоуправления, располагающих такого рода информацией, предоставлять ее по соответствующим запросам. Возможные исключения из этого общего правила должны обязательно иметь форму федерального закона (ч. 3 ст. 55 Конституции РФ). Ст. 42 Конституции РФ говорит о праве каждого на достоверную информацию о состоянии окружающей среды. Ст. 19 Основ законодательства РФ "Об основах охраны здоровья граждан Российской Федерации" конкретизирует это установление закреплением определенного механизма реализации прав граждан на информацию о факторах, влияющих на их здоровье (п.5 пп.7 ст. 19).[8]

Федеральный закон № 149-ФЗ - назначение закона обеспечение защиты информации, регулирования отношений при осуществлении права на поиск,

---

[8] Струков В.И. Правовое обеспечение защиты информации, часть 1: Учебно-методическое пособие. Таганрог: Изд-во ТТИ ЮФУ 2019 С.45

получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений в области охраны результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Качество современного уровня правового регулирования отношений по поводу информации во многом определяется степенью учета законодателем этих признаков (свойств).

Конфиденциальная информация определена в п. 7 ст. 2 Федерального закона № 149-ФЗ через требование не передавать такую информацию третьим лицам без согласия ее обладателя. На мой взгляд, это определение небезупречно. Вряд ли можно согласиться с определением конфиденциальной информации опять-таки через информацию с ограниченным доступом, не содержащую государственную тайну, во-первых, потому, что такое определение оказывается в замкнутом круге: нельзя определять подобное подобным; во-вторых, государственная тайна - это тоже конфиденциальная информация. Поэтому более правильно, на мой взгляд, под конфиденциальной информацией понимать легально полученную информацию, которая в силу закона или иного акта, имеющего юридическое значение, доступна строго определенному кругу лиц, и в отношении которой установлен режим той или иной степени секретности.

Пункт 3 статьи 5 Федерального закона № 149-ФЗ содержит классификацию информации в зависимости от порядка ее предоставления или распространения. Так, по этому основанию информация подразделяется:

1) на информацию, свободно распространяемую, например, посредством средств массовой информации;

2) на информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) на информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) на информацию, распространение которой в Российской Федерации ограничивается или запрещается. Например, информация, составляющая коммерческую или государственную тайну.

В п. 2 этой статьи приводится разделение информации в зависимости от категории доступа к ней. По этому основанию информация может быть общедоступной; ограниченного доступа.

Федеральным законом № 152-ФЗ регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими и физическими лицами с использованием средств автоматизации или без их использования, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием

средств автоматизации.

ФСТЭК предлагает выделять персональные данные из информационных систем, содержащих информацию ограниченного доступа и защищаемых в режиме тайны, что во многих случаях не реализуемо. Выделение персональных данных из общего массива охраняемой информации создает для оператора проблему соотношения требований по технической защите информации, а также проблему соотношения прав и обязанностей субъектов в отношении защищаемой информации.

С 1 января 2008 года в силу вступила часть четвертая Гражданского кодекса Российской Федерации (далее – ГК РФ), регулирующая отношения по поводу результатов интеллектуальной деятельности. Введены понятия "секрет производства" (ст. 1465 ГК РФ: секретом производства (ноу-хау) признаются сведения любого характера (технические, производственные, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа, на законном основании, и в отношении которых обладателем таких сведений введен режим коммерческой тайны) и "служебные секреты производства" (ст. 1470 ГК РФ: исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю. Гражданин, которому в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства).

Что касается служебных секретов производства, то исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, принадлежит работодателю. Но существует и важная особенность: на работника возлагается обязанность сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства независимо от того, создал ли такой работник результат интеллектуальной деятельности или соответствующие сведения стали известны работнику лишь в связи с выполнением своих служебных обязанностей.[9]

Федеральный закон№ 98-ФЗ, Федеральный закон№ 149-ФЗи часть 4 ГК РФ - ввели, как говорилось выше, и новые понятия, и изменили содержание некоторых прежних понятий, относящихся к данному вопросу. Ст. 139 ГК

---

[9]Снытников, А.А. Обеспечение и защита права на информацию // А.А. Снытиков, Л.В. Туманова. М.: "Городец-издат" 2019 С. 34-35.

РФ, определявшая коммерческую тайну, отменена.

В ст. 3 Федерального Закона № 98-ФЗ определяется как режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Федеральный закон от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи"(Федеральный закон№ 63-ФЗ)- данный закон призван обеспечить конфиденциальность информации в электронном виде - подписи, которая рассматривается как личная подпись субъекта.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ"О техническом регулировании" - закон призван обеспечить защиту сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, продукции (работ, услуг) и объектов, для которых устанавливаются требования, связанные с обеспечением ядерной и радиационной безопасности в областииспользования атомной энергии, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения указанной продукции и указанных объектов.

Иные федеральные законы в том или ином аспекте также могут регулировать деятельность, касающуюся информации, информационных технологий и защиты информации. Так, глава 13 Кодекса РФ об административных правонарушениях № 195-ФЗ от 30 декабря 2001 г. (далее – КоАП РФ) устанавливает ответственность за административные правонарушения в области связи и информации.

В соответствии с Законом РФ от 27.12.1991 N 2124-1 "О средствах массовой информации"поиск, получение, производство и распространение массовой информации, учреждение ее средств, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации, не подлежат ограничениям, за исключением предусмотренных соответствующим законодательством РФ.

В числе нормативных правовых актов, частично регулирующих рассматриваемые отношения, следует назвать также Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации". Пользователь архивных документов имеет право использовать, передавать, распространять информацию, содержащуюся в них, а также копии архивных документов для любых законных целей и любым законным способом. Кроме того, приняты и иные нормативные правовые акты в данной области.

Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" - указ призван

обеспечить защиту информации путем создания Федеральной службой по техническому и экспортному контролю своих территориальных органов, Государственного научно-исследовательского испытательного института проблем технической защиты информации.

Указ Президента РФ от 20.01.1994 N 170 "Об основах государственной политики в сфере информатизации" установил, что основными направлениями государственной политики в сфере информатизации являются: обеспечение единства государственных стандартов в сфере информатизации, их соответствие международным рекомендациям и требованиям. Указ Президента Российской Федерации № 188 от 6 марта 1997 г. установил перечень сведений конфиденциального характера.

Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности"- данное постановление регламентирует порядок обращения и работы с конфиденциальной информацией федеральными органами исполнительной власти с целью предотвращения угрозы утечки информации и обеспечения защиты информации.

Постановление Правительства РФ от 26.06.1995 N 608 "О сертификации средств защиты информации" - данное Постановление утвердило Положение об обязательной сертификации средств защиты информации, где отражен порядок сертификации средств защиты информации в Российской Федерации.

Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления ее обеспечения и служит основой для формирования государственной политики и подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, а также для разработки ее целевых программ.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся: достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания; свобода массовой информации; неприкосновенность частной жизни, личная и семейная тайна; русский язык как фактор духовного

единения народов многонациональной России, язык межгосударственного общения народов государств - участников Содружества Независимых Государств; языки, нравственные ценности и культурное наследие народностей Российской Федерации; объекты интеллектуальной собственности.

Российская Федерация является участником международных договоров, касающихся информации, информационных технологий и защиты информации. Общее число тайн превысило 40, а термин "конфиденциальность" встречается в 84 федеральных законах и 706 международных актах, в том числе в межправительственных соглашениях. В качестве примеров можно привести следующие документы: Европейская Конвенция об информации относительно иностранного законодательства (ETS № 62) (заключена в Лондоне 7 июня 1968 г.); Соглашение о межгосударственном обмене научно-технической информацией и Соглашение об обмене экономической информацией (заключены в Минске 26 июня 1992 г.); Соглашение о сотрудничестве в области информации (заключено в Бишкеке 9 октября 1992 г.); Соглашение об обмене информацией в области внешнеэкономической деятельности (заключено в Москве 24 сентября 1993 г.); Конвенция о сотрудничестве в области культуры, образования, науки и информации в Черноморском регионе (заключена в Стамбуле, 6 марта 1993 г.); Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации (заключено в Москве, 24 декабря 1999 г.); Конвенция о преступности в сфере компьютерной информации (ETS N 185) (заключена в Будапеште 23 ноября 2001 г.); Соглашение между Министерством информационных технологий и связи Российской Федерации и Министерством экономики и труда Федеративной Республики Германия о сотрудничестве в области информационных технологий и связи (заключено в Ганновере 11 апреля 2005 г.); Соглашение между Правительством Российской Федерации и Правительством Союза Мьянма о взаимной защите секретной информации (заключено в Москве 3 апреля 2006 г.) и др.

Подводя итог по Главе I. можно сделать вывод, что конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную, профессиональную или личную тайны, охраняющиеся её владельцем.

Отношения по поводу информации в целом и конфиденциальной информации в частности, регулируются правом. При этом информация как таковая и конфиденциальная информация являются предметом регулирования различных отраслей права и нормативных правовых актов РФ, важнейшее место среди которых занимает Конституция РФ.

ГЛАВА II. АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ СОВЕРШЕНИЮ ПРАВОНАРУШЕНИЙ В СФЕРЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1. Общая характеристика и виды правонарушений в сфере защиты конфиденциальной информации

Можно выделить следующие направления возможных правонарушений в отношении конфиденциальной информации, обрабатываемой в автоматизированных системах:

1) уничтожение или искажение информации;
2) несанкционированный доступ (получение, хищение);
3) несанкционированное размножение;
4) несанкционированное использование;
5) несанкционированная модификация;
6) несанкционированное блокирование;
7) другие нарушения.

Эти направления можно использовать как вариант оснований классификации возможных правонарушений в отношении конфиденциальной информации.

В ходе организации защиты компьютерной информации нужно учитывать следующие особенности законодательства об ответственности при работе с информацией:

-необходимость четкого выявления предмета противоправного действия;

-доказательность противоправного действия;

-адресность действия и возможность выявления конкретного правонарушителя.

Конституция РФ выделяет три субъекта права: человек (личность), общество и государство. Соответственно и правонарушения в информационной сфере подразделяются на преступления против личности, общества и государства.

Анализ возможных противоправных действий позволяет выявить ряд их составов:

•шпионаж, разглашение сведений, утрата носителей сведений - нарушение государственной тайны;

•промышленный шпионаж - нарушение коммерческой тайны;

•несанкционированный сбор, использование персональных данных, непредставление данных - нарушение профессиональной или личной тайны.

Правонарушения могут быть:

-имущественными (например, незаконное использование данных);

-"технологическими" (несанкционированное копирование данных; искажение и модификация данных и программ; распространение компьютерных вирусов; нарушение технологии обработки данных; проникновение в автоматизированные информационные системы в "обход"

механизмов защиты).[10]

В силу неоднозначности самого понятия и содержания информации, в том числе подлежащей защите, существуют неопределенности понятия и содержания характеристик правонарушений в области информационной безопасности.

Один из вариантов субъективного определения содержания таких характеристик включает признаки, характеризующие состояние системы защиты конфиденциальной информации (оперативная обстановка, структура, динамика правонарушений), а также причины правонарушений, каналы утечки, методы, способы, средства, меры предупреждения правонарушений и др.

Согласно Российскому законодательству за правонарушения в сфере защиты информации определены следующие виды ответственности:

Уголовная,

Административная,

Гражданско-правовая,

Дисциплинарная.

Федеральный закон № 149-ФЗ:

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации:«Нарушение требований настоящего закона влечет за собойдисциплинарную, гражданско-правовую, административную или уголовнуюответственность в соответствии с законодательством Российской Федерации.

КоАП устанавливает ответственность за следующие правонарушения:

-Нарушение условий, предусмотренных лицензией на осуществлениедеятельности в области защиты информации (за исключением информации,составляющей государственную тайну);

-Использование несертифицированных информационных систем, баз ибанков данных, а также несертифицированных средств защиты информации,если они подлежат обязательной сертификации (за исключением средствзащиты информации, составляющей государственную тайну);

-Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключениеминформации, составляющей государственную тайну);

-Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну),

-Занятие видами деятельности в области защиты информации (заисключением информации, составляющей государственную тайну) безполучения в установленном порядке специального разрешения (лицензии), еслитакое разрешение (такая лицензия) в соответствии с федеральным закономобязательно (обязательна).

---

[10] Данилов А.Д. Ценность информации // Технологии информационного общества. 2018. № 10. С. 127-130.

Уголовный кодекс РФ(далее – УК РФ) предусматривает следующие виды ответственности за преступления в области защиты информации:

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Предмет преступления включает сведения, составляющие коммерческую, налоговую или банковскую тайну. Понятие и признаки коммерческой тайны предусмотрены ст. 3 и 5 Федерального закона № 98-ФЗ. Определение налоговой тайны дано в ст. 102 Налогового кодекса РФ (далее – НК РФ). Содержание банковской тайны раскрывается в ст. 857 ГК РФ и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 "О банках и банковской деятельности".

2. Объективная сторона в ч. 1 выражается в собирании сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом. Под собиранием следует понимать умышленные действия, направленные на получение составляющих тайну сведений любыми незаконными способами.

3. В ч. 2 сформулировано два альтернативных состава преступления. Под незаконным разглашением следует понимать сообщение или любую иную передачу составляющих тайну сведений лицу, не имеющему к ним доступа на законном основании. Под незаконным использованием следует понимать использование составляющих тайну сведений в целях, не связанных с теми, для реализации которых лицу предоставлен доступ к сведениям.

4. Момент окончания преступления определяется для собирания как момент начала получения хотя бы части таких сведений; для незаконного разглашения как момент сообщения или иной передачи сведений лицу, не имеющему к ним доступа на законном основании; для незаконного использования как момент начала применения сведений в целях, не связанных с теми, для реализации которых лицу предоставлен к ним доступ.

5. Крупный ущерб состоит в причинении убытков владельцу тайны в виде реального ущерба (например, утраты права на результат интеллектуальной деятельности) и (или) в виде упущенной выгоды (например, неполученных доходов вследствие утраты конкурентного преимущества, основанного на коммерческой тайне).

Тяжкие последствия как оценочный признак выражаются в наступлении иных последствий (например, прекращение деятельности предприятия, массовое увольнение персонала и т.п.).

6. Собирание или незаконное использование сведений, составляющих коммерческую, налоговую или банковскую тайну, в рамках подготовки или совершения кражи, мошенничества или присвоения чужого имущества поглощается соответствующими составами преступлений против собственности и не требует самостоятельной квалификации по ст. 183 УК РФ.

7. С субъективной стороны преступления характеризуются прямым или

косвенным умыслом. В отношении крупного ущерба и тяжких последствий также возможна неосторожная форма вины.[11]

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Примечание. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

1. Создание, распространение или использование компьютерных программлибо иной компьютерной информации, заведомо предназначенных длянесанкционированного уничтожения, блокирования, модификации,копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Статья 274. Нарушение правил эксплуатации средств хранения, обработкиили передачи компьютерной информации и информационно-телекоммуникационных сетей.

1. Нарушение правил эксплуатации средств хранения, обработки или

передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшееуничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Также, уголовной ответственности подлежит незаконное собирание илираспространение сведений о частной жизни лица, составляющих его личнуюили семейную тайну, без его согласия либо распространение этих сведений впубличном выступлении или в средствах массовой информации. Отягчающим обстоятельством по данномувиду нарушений признается данное правонарушение, совершенное сиспользованием своего служебного положения.

Также к уголовной ответственности могут быть привлечены лица,оказывающие услуги по технической защите информации и не имеющиесоответствующей лицензии, либо осуществляющие деятельность снарушением лицензионных требований и условий, если это деяние причинилокрупный ущерб гражданам, организациям или государству, либо сопряжено сизвлечением дохода в крупном размере. Речь идет обуголовной ответственности по статье 171 УК РФ.

Отягчающим признаком по данной статье признается совершениепреступления организованной группой лиц, либо сопряженное с

---

[11] "Комментарий к Уголовному кодексу Российской Федерации" (постатейный) (9-е издание, переработанное и дополненное) (под ред. Г.А. Есакова) ("Проспект", 2021). С. 15-18.

извлечением дохода в особо крупном размере.

Виновные в нарушении требований нормативно-правовых документов позащите информации также подлежат гражданско-правовой ответственности вслучае нанесения материального ущерба потерпевшей стороне. Так какспецифика гражданско-правовых отношений, характеризующихся равенствомучастников, предопределяет особенности гражданско-правовойответственности, которая выступает одной из разновидностей юридическойответственности. Главной из этих особенностей является имущественныйхарактер принудительных мер воздействия на правонарушителя.

Также в трудовом кодексе РФ предусмотрена дисциплинарнаяответственность за нарушения правил защиты информации в организациикак за любое другое нарушение трудовой дисциплины.[12]

Федеральный закон от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" (далее - Федеральный закон № 79- ФЗ) устанавливает обязанность для государственных служащих, которая содержит в себе запрет на разглашение гражданским служащим сведений, составляющих государственную и иную охраняемую федеральным законом тайну, а также сведений, ставших ему известными в связи с исполнением должностных обязанностей, в том числе сведений, касающихся частной жизни и здоровья граждан или затрагивающие их честь и достоинство (79-ФЗ п. 7 ч. 1 ст. 15).

К таким сведениям относятся сведения, составляющие государственную тайну, служебную тайну, налоговую тайну, коммерческую тайну, персональные сведения, сведения конфиденциального характера.

Обсуждение запрета, предусмотренного п. 9 ч. 1 ст. 17 Федеральный закон№ 79-ФЗ, в исследованиях, как правило, начинается с указания на конституционное право граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ). Согласно ч. 1 ст. 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2.2. Механизмы выявления правонарушений в сфере защиты конфиденциальной информации в рамках служебных полномочий

Согласно ч. 4 ст. 6 Федерального закона № 149-ФЗ обладатель информации обязан принимать меры по ее защите.

К числу таких мер относятся правовые, организационные и

[12] Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. 2011. № 4. С.25-30.

технические. Их целью является:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализация права на доступ к информации.[13]

Обладателями подлежащей защите информации являются организации и физические лица, Российская Федерация, субъект РФ, муниципальное образование.

В соответствии с п. 7 ст. 2Федерального закона № 149-ФЗ под конфиденциальностью информации понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Следовательно, конфиденциальной информацией является та, в отношении которой установлены соответствующие требования о неразглашении.

Согласно п. 1 ст. 3 Федерального закона № 98-ФЗ в отношении организаций под конфиденциальной принято понимать информацию, составляющую коммерческую тайну.

Частью 1 ст. 10Федерального закона № 98-ФЗ предусмотрены следующие меры по защите конфиденциальной информации:

- определение перечня информации, составляющей коммерческую тайну;

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и/или лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для организаций - полное наименование и место нахождения, для индивидуальных предпринимателей - их фамилия, имя, отчество и место жительства).

Порядок работы с конфиденциальной информацией в рамках гражданско-правовых отношений стороны согласовывают в подписываемых

---

[13] Степанов Е.А. Информационная безопасность и защита информации: учебное пособие // Е.А. Степанов, И.К. Корнеев. М.: Инфра-М. 2019. С. 33-36.

ими договорах, соглашениях и иной документации, подписание и обмен которой осуществляются в процессе их сотрудничества.

Для обеспечения конфиденциальности информации сотрудниками организации, доступ которых к конфиденциальной информации необходим для исполнения ими своих трудовых обязанностей, применяются следующие правила:

- соответствующий работник должен быть под расписку ознакомлен с перечнем информации, составляющей коммерческую тайну, режимом коммерческой тайны и с мерами ответственности за его нарушение;

- работникам должны быть созданы необходимые условия для соблюдения ими режима коммерческой тайны.

Дополнительные условия о неразглашении такой информации могут быть предусмотрены в трудовом договоре (ст. 57 Трудового кодекса РФ).

Защита персональных данных оператором персональных данных субъекта.

В соответствии со ст. 3 Федерального закона № 152-ФЗ субъектом персональных данных является физическое лицо, а персональными данными - любая информация, прямо или косвенно его индивидуализирующая.

Оператором согласно указанной норме является государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.[14]

На оператора персональных данных субъекта возлагается обязанность по их защите.

В качестве мер защиты ч. 2 ст. 19Федерального закона № 152-ФЗ предусмотрено:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

-оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

---

[14]Кнопкин Н. Защита персональных данных: антикризисный подход // IT-manager. 2016. № 6. С. 23.

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

-восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

-установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Помимо этого, оператор должен:

- назначить ответственного за организацию обработки персональных данных;

- издать документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- производить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Законом;

- знакомить своих работников, непосредственно осуществляющих обработку персональных данных, с положениями российского законодательства о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Специальные требования к защите персональных данных установлены также:

- главой 14 Трудового кодекса РФ;

- Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных";

- Приказом ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

- Приказом ФСБ России от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".[15]

Для того чтобы не произошла утечка конфиденциальной информации, необходимо предпринимать соответствующие меры, которые препятствовали бы этому.

Также существует несколько правовых способов защиты сведений ограниченного доступа. Законодательное регулирование по вопросам, связанным с защитой сведений ограниченного доступа, заключается также в закреплении юридической ответственности за разглашение такой информации.

Как упоминалось выше, положения, регламентирующие вопросы по защите конфиденциальной информации, закреплены в Федерального закона № 149-ФЗ. В соответствии с законодательством, под защитой информации понимается:

-обеспечение защиты сведений ограниченного доступа от неправомерного посягательства;

-соблюдение режима ограниченного доступа к ограниченным данным;

-принятие мер по реализации права на доступ к ограниченной информации.

Законодательное координирование данных ограниченного доступа заключается также в том, чтобы принять меры по защите информации:

-предотвращение утечки информации;

-своевременное обнаружение попытки незаконно получить доступ к информации;

-предупреждение последствий, которые возникают при несанкционированном доступе к сведениям;

-постоянный мониторинг уровня защиты информации;

-возможность восстановить данные, которые были уничтожены;

-размещение информации ограниченного доступа в базах данных на территории РФ.

Для защиты критичных данных существуют следующие виды защиты:

---

[15] Лопатин, В.Н. Правовая охрана и защита права на тайну / В.Н. Лопатин // Юридический мир. 2019. №7. С.36 - 37.

Физическая. Физическая защита заключается в хранении информации в специальных сейфах или хранилищах, доступ к которым разрешен узкому кругу лиц. Обеспечение внутриобъектового режима объекта информатизации.

Аппаратная. Аппаратный способ защиты предполагает хранение информации на специальных компьютерах или серверах, которые постоянно контролируются с целью предотвращения несанкционированного доступа к данным.

Программная. Защита информации осуществляется с помощью программного обеспечения, которое своевременно блокирует неразрешенные действия пользователей и предотвращает утечку сведений.

Математическая (криптографическая). Математическая защита позволяет шифровать данные, делая их прочтение недоступным для третьих лиц.[16]

Вопросы сохранности конфиденциальных данных не сходят с повестки дня уже несколько лет. Главный вопрос в условиях глобализации и цифровизации— как защитить конфиденциальную информацию от посторонних?

Я считаю, что технические средства не могут в полной мере решить проблему утечки и сохранности конфиденциальной информации. Только определенная дисциплина и культура среди сотрудников может предотвратить утечку и разглашение конфиденциальной информации.

Согласно последним исследованиям, три из пяти главных причин утечек информации связаны с действиями людей: это и случайные утечки, спровоцированные сотрудниками (8% случаев), и утечки с мобильных устройств работников (7%), и так называемый корпоративный шпионаж (7%).

Утечки информации из организации бывают как преднамеренные, так и непреднамеренные, при этом вне зависимости от типа большинство из них остаются незамеченными. Одни из самых частых — случайные, происходящие по вине внутренних сотрудников организаций. Чаще всего работники невнимательны при отнесении той или иной информации к конфиденциальной, в связи с чем возникает угроза конфиденциальности информации, обсуждают внутренние служебные вопросы за пределами места работы или службы, теряют внутренние документы.

Преднамеренные утечки информации по вине сотрудников также распространены. Часто это плохо спланированные или эмоциональные действия: например, месть руководству или коллегам, обида за понижение в должности и другие. Как правило, такие преступления легко раскрываются — найти виновного сотрудника довольно просто: его выдают либо оставленные в спешке улики, либо явный мотив.

---

[16] Степанов Е.А. Информационная безопасность и защита информации: учебное пособие // Е.А. Степанов, И.К. Корнеев. М.: Инфра-М. 2018. С. 89-90.

Гораздо сложнее вычислить нечистого на руку сотрудника — того, кто целенаправленно и последовательно «крадет» или «сливает» конфиденциальную информацию.

Например, он собирается сменить место работы, поэтому «уводит» из организации информацию необходимую для успешного продвижения на новом месте работы. В случае с сотрудниками налоговых органов, такой сотрудник может вступать в сговор с проверяемыми налогоплательщиками и может «сливать» им информацию необходимую для ухода от ответственности за налоговые правонарушения и соответственно получать за это определенное вознаграждение.

В случаи реальной утечки и разглашении конфиденциальной информации, для установления правонарушителя необходимо сузить круг лиц по имеющим доступ к информации которая подверглась разглашению, при установлении правонарушителя необходимо обратить внимание на его поведение: потенциального правонарушителя выдает нервозность. Необходимо установить наличие конфликтов сотрудника с руководством, планы по увольнению из организации и потенциальнуюаффилированность с лицами которые позже использовали данную информацию.

Считаю хорошим метод предотвращение утечек конфиденциальной информации — проведение сотрудником по информационной безопасности постоянной разъяснительной и ознакомительной работы с сотрудниками на предмет запрета неправомерного разглашения конфиденциальной информации, по порядку работы с информацией ограниченного доступа и по вопросу установленной ответственности за разглашение конфиденциальной информации.

Каждый работник должен понимать, какие данные конфиденциальные и как с ними обращаться.

Так жекрайне эффективный метод по предупреждению правонарушений в области защиты конфиденциальной информации - показательные наказания.

Ощущение неизбежности наказания и страх перед ним — это отличный мотиватор для того, чтобы не нарушать правила работы с информацией.

Проблему обеспечения безопасности конфиденциальной информации только надзорными методами решить невозможно.

Предусмотренные в настоящий момент штрафы не стимулируют соблюдать законодательство, а незаконное вознаграждение за предоставление такой информации может значительно превышать предусмотренный штраф.

Я полагаю, что крайне жестко нужно подходить к ответственности за правонарушения в области защиты конфиденциальной информации, нужна жесточайшая административная и уголовная ответственность, иначе исключить или хотя бы минимизировать правонарушения в области защиты конфиденциальной информации не получится.

2.3. Особенности защиты конфиденциальной информации ФНС России. Проблемы и пути совершенствования системы защиты конфиденциальной информации

Главной целью обеспечения безопасности информации в ФНС России является предотвращение или минимизация ущерба (прямого или косвенного, материального, репутационного или иного) субъектам правоотношений посредством деструктивного воздействия на информацию, обрабатываемую в ФНС России, ее носителям и технологическим процессам обработки информации.

Основными целями обеспечения безопасности информации являются:

- выполнение требований законодательства в сфере обеспечения безопасности информации, в том числе нормативных правовых актов ФСТЭК России и ФСБ России;
- предотвращение несанкционированного доступа к информации и техническим средствам, используемым для ее обработки;
- обеспечение доступности информации и предотвращение последствий нарушения порядка доступа к ней;
- предотвращение нарушений прав субъектов при обработке информации;
- недопущение деструктивного воздействия на информацию.

Основными задачами, вытекающими из целей обеспечения безопасности информации в ФНС России, являются:

- выявление угроз ИБ и определение вероятности их реализации (актуальности), управление рисками ИБ;
- совершенствование политики ИБ ФНС России при создании и внедрении ИС ФНС России;
- обеспечение соответствия мер и средств защиты информации в налоговых органах и подведомственных организациях ФНС России положениям нормативных документов по безопасности информации;
- совершенствование нормативных правовых актов и организационно-распорядительных документов ФНС России в области обеспечения ИБ, координация деятельности налоговых органов по защите информации;
- информационная поддержка принятия управленческих решений по вопросам информационной безопасности ЦА ФНС России, создание системы управления информационной безопасностью;
- защита от вмешательства в процесс функционирования информационных систем ФНС России посторонних лиц, совершенствование СОБИ, ее организации, форм и методов предотвращения и нейтрализации угроз ИБ, ликвидации последствий их реализации;
- предотвращение, в том числе с использованием организационно-правовых мер и технических средств защиты информации, несанкционированных действий и незаконных посягательств на активы информационной безопасности налоговых органов и подведомственных организаций ФНС России со стороны посторонних лиц и пользователей ИС ФНС России, не имеющих соответствующих полномочий;

- регистрация событий, влияющих на безопасность информации, оперативный анализ информации о таких событиях и своевременное выявление инцидентов ИБ и реагирование на них, обеспечение полной подконтрольности и подотчетности выполнения всех операций, совершаемых в ИС налоговых органов;

- обеспечение возможности восстановления актуального состояния ИС ФНС России при нарушении ИБ.[17]

Защита информации ограниченного доступа (распространения), представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации;

3) реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

Информация не может быть рассмотрена в отрыве от элементов инфраструктуры ИС ФНС России (объекта информатизации), на которых она обрабатывается (хранится, обсуждается), поэтому точкой приложения усилий по защите ИР является инфраструктура ИС налоговых органов (объекты информатизации), в том числе:

помещения, здания, объекты, сооружения, передвижные объекты ФНС России, предназначенные для работы с информацией;

оборудование ИС (серверные комплексы, рабочие станции пользователей, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных, программно-аппаратные средства удостоверяющего центра, источники бесперебойного питания);

телекоммуникационные сети и системы (активное и пассивное коммуникационное оборудование, система управления, мониторинга и обслуживания инфраструктурой);

средства и системы связи и передачи данных (ведомственной, междугородней, городской, внутренней);

программные средства (операционные системы, системы управления базами данных, другое общесистемное, специальное и прикладное программное обеспечение);

средства защиты информации (далее – СЗИ);

технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

---

[17] Кучеров И.И. Налоговая тайна в системе мер защиты конфиденциальной информации / Налоговое право России: учебник / отв.ред. Ю.А. Крохина. - 6-е изд., испр. - М.: Норма, 2021. С. 55.

документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);

средства обеспечения жизнедеятельности объектов (гарантированные и бесперебойные системы электропитания и заземления объектов, системы пожарной и охранной сигнализации, электронные системы контроля и управления доступом на территорию и в помещения, системы громкоговорящей связи и оповещения, системы кондиционирования, отопления, вентиляции и пожаротушения).

При обработке информации ограниченного доступа в ФНС России необходимо обеспечивать специальные условия хранения, обработки и обращения документов, содержащих информацию ограниченного доступа, гарантирующие надежную защиту как самих документов (материальных носителей), так и содержащейся в них конфиденциальной информации. Это обеспечивается следующими мероприятиями:

- введена персональная ответственность сотрудников налоговых органов и подведомственных ФНС России организаций за учет, сохранность конфиденциальных документов и порядок обращения с ними;

- разработана в ФНС России регламентированной технологии издания и обработки конфиденциальных документов, в том числе на стадии подготовки черновиков и проектов документов, определением состава издаваемых документов и содержащейся в них конфиденциальной информации, включающей (но не ограничиваясь):

- определен порядок работы с документами ограниченного доступа в специально выделенных помещениях ФНС России, налоговых органов и подведомственных ФНС России организаций;

- определен порядок передачи документов ограниченного доступа в случае ухода сотрудника ЦА ФНС России, налоговых органов и подведомственных организаций ФНС России в отпуск, командировку, при увольнении и т.д.;

- определен порядок пересылки документов ограниченного доступа, создание реестровой системы передачи конфиденциальных документов;

- созданы архивы документов ограниченного доступа, проводится регулярная экспертиза ценности документов и оценки возможности снятия отметки грифа конфиденциальности;

- определен порядок уничтожения документов ограниченного доступа;

- в ФНС России введены требования к условиям хранения документов ограниченного доступа и обращения с ними:

- обязательный поэкземплярный и полистной учет всех документов, содержащих сведения ограниченного доступа, а также проектов и черновиков таких документов;

- определение полного состава регистрационных данных о каждом документе, содержащем сведения ограниченного доступа (дата создания, получения, исполнения; регистрационный номер; фамилия, имя, отчество (при наличии) исполнителя, адресата; права доступа; степень конфиденциальности; количество листов и т.д.);

- организация системы фиксации движения и местонахождения документов ограниченного доступа в ЦА ФНС России, налоговых органах и подведомственных организациях ФНС России;

- организация хранения конфиденциальных документов на рабочих местах сотрудников ЦА ФНС России, налоговых органов и подведомственных организаций ФНС России;

- организация хранения документов ограниченного доступа в архивах ЦА ФНС России, налоговых органов и подведомственных организаций ФНС России;

- созданием в ФНС России разрешительной системы доступа к документам ограниченного доступа и делам, обеспечивающей правомерное и санкционированное ознакомление с ними:

- разделение документов по степени конфиденциальности;

- присвоение каждому документу грифа конфиденциальности;

- разграничение права работы с документами ограниченного доступа;

- запрет несанкционированного выноса документов ограниченного доступа;

- принятие организационных мер, исключающих необоснованное ознакомление с документами сотрудников ЦА ФНС России, налоговых органов и подведомственных организаций ФНС России, не имеющих полномочий;

- проведение руководителями подразделений ЦА ФНС России, налоговых органов и подведомственных организаций ФНС России систематических проверок наличия конфиденциальных документов у исполнителей.

Виды угроз безопасности конфиденциальной информации:

1) угрозы нарушения конфиденциальности:

хищение (утечка, перехват, съем) информации и средств ее обработки;

утрата (неумышленная потеря) информации, средств ее обработки;

разглашение информации;

2) угрозы нарушения целостности информации:

модификация (искажение) информации;

отрицание подлинности информации;

навязывание ложной информации;

3) угрозы нарушения доступности информации:

блокирование информации;

уничтожение информации и средств её обработки и хранения.[18]

Все нарушители делятся на две основные группы: внутренние и внешние.

---

[18] Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз // Вестник компьютерных и информационных технологий. — 2018. — № 8(122). С. 48-53.

Под внутренними потенциальными нарушителями подразумеваются работники ФНС России, имеющие санкционированный доступ конфиденциальной информации.

Под внешними потенциальными нарушителями подразумеваются все остальные лица.

Возможный ущерб от нарушения безопасности конфиденциальной информации:

материальный (экономический) ущерб любому субъекту от разглашения информации, являющейся объектом защиты;

моральный вред, материальный ущерб любому субъекту персональных данных, от их разглашения или нарушения конституционных прав и свобод граждан;

материальный ущерб от необходимости восстановления любым субъектом нарушенных прав и объектов защиты;

моральный вред, материальный ущерб от дезорганизации деятельности ФНС России;

материальный ущерб ФНС России от уничтожения (утраты) объектов защиты;

материальный ущерб, моральный вред от несвоевременного поступления информации потребителям государственных информационных услуг или от нарушения целостности предоставленной информации;

материальный ущерб от невозможности выполнения ФНС России обязательств перед третьей стороной.

Среди методов противодействия и предотвращения правонарушений в области защиты конфиденциальной информации выделим следующие основные группы:

правовые методы;

экономические методы;

организационные методы;

инженерно-технические методы;

технические методы;

программно-аппаратные методы.

Для развития ИС ФНС России могут привлекаться внешние специализированные организации - поставщики услуг. Деятельность по обслуживанию ИС ФНС России, передаваемая для выполнения другой организации должна учитывать требования настоящей по защите информации.

В случае аутсорсинга регламентация вопросов ИБ носит обязательный характер, поскольку зоны полномочий и ответственности должны быть определены заранее, и в случае инцидента нужно четко идентифицировать ответственных и определить виновных.

Требования безопасности, в случае, когда ФНС России передает для управления и контроля все или некоторые из элементов ИТ-инфраструктуры ФНС России, должны быть указаны в контракте (или ином документе), согласованном между сторонами и учитывающем:

- наличие соглашения о неразглашении поставщиком услуг информации ограниченного доступа/распространения, ставшей известной ему в ходе исполнения договорных обязательств;

- выполнение требований по защите информации, установленные законодательством Российской Федерации;

- достижение зафиксированных договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности;

- возможность обеспечения и тестирования параметров целостности, доступности и конфиденциальности ИР ФНС России;

- уровни физической безопасности, которые должны быть обеспечены в отношении оборудования, используемого в рамках аутсорсинга;

- соблюдение поставщиком услуг требований законодательства Российской Федерации о лицензировании, сертификации, а также требований трудового законодательства;

- право на проведение аудита деятельности поставщика услуг со стороны ФНС России;

- возможность расторжения договора с внешней организацией в одностороннем порядке;

- необходимость разработки регламента доступа ФНС России к арендуемым мощностям и каналам связи;

- необходимость разработки регламента информирования ФНС России о попытках НСД при использовании арендуемого оборудования и каналов связи;

- необходимость выполнения технических требований по защите информации, действующих в ФНС России;

- обеспечения отдельных правил информационной безопасности в случае приобретения, разработки и эксплуатации информационных систем.

Пресечение угроз при обработке информации ограниченного доступа (распространения) на файловых северах и серверах, содержащих отдельные базы данных, обеспечивается:

- использованием защищенных версий протоколов для передачи информации;

- мониторингом информационных потоков в элементах сетевой инфраструктуры АИС ФНС России;

- осуществлением разграничения доступа работников ФНС России и подведомственных организаций к информации на файловых серверах в соответствии с установленными полномочиями, как за счет использования комплекса организационно-технических, так и программно-аппаратных средств защиты.

Нарушение установленного порядка разграничения доступа может произойти как неумышленно - за счет воздействия вирусов или спама, так и за счет умышленных действий пользователей.

Защита от вирусов и спама осуществляется в рамках общей антивирусной системы защиты информации при её обработке с использованием СВТ в ФНС России.

Защита от злонамеренных действий пользователей, осуществляется введением запрета на:

- использование иных, не входящих в утвержденное ПО программ, позволяющих изменять установленные права доступа;
- подключение к техническим устройствам, осуществляющим обработку информации, средств и устройств, не входящих в утвержденную к применению конфигурацию технических средств и устройств.

Для осуществления необходимого уровня ИБ и контроля за состоянием ИБ при защите конфиденциальной информации на файловых серверах, необходимо дополнительно использовать комплекс организационно-технических мер, осуществляющий мониторинг:

действий пользователей и процессов автоматической обработки информации;

целостности ПО;

целостности конфигурации ПО и технических средств, предназначенных для обработки информации.

На сегодняшний день возникает угроза утечки информации из-за введенных в результате пандемии COVID-19 ограничительных мер.

Так, многие организации в том числе и налоговые органы, переводят сотрудников на дистанционную работу, не обеспечив должным образом сохранность конфиденциальной информации.

Основным сценарием дистанционной работы является удаленное подключение пользователя из дома к непосредственно своей служебной рабочей станции, для исполнения возложенных на него служебных обязанностей.

Мероприятия которые проводятся при переводе сотрудника на дистанционную работу:

-издается приказ о переводе сотрудника на удаленную работу;

-проводится внеочередной инструктаж по информационной безопасности, в том числе с разъяснением порядка работы в дистанционном режиме;

-сотрудником который подлежит переводу на дистанционную работу предоставляется обязательство о неразглашении информации полученной в рамках исполнения должностных обязанностей;

-производится настройка защищенного подключения междуслужебной рабочей станций и ПК для удаленной работы.

Вышеперечисленные технические и организационно-распорядительные меры не обеспечивают должным образом информационную безопасность, в том числе достаточную защиту конфиденциальной информации налоговых органов.

В таких условиях могут возникать угрозы информационной безопасности и факты правонарушений связанных с защитой

конфиденциальной информации. Они возможны, так как имеют место быть следующие обстоятельства:

-недостаточная защита конечных устройств пользователей, в том числе возможны случаи их утраты, хищения;

-недостаточно строгие политики информационной безопасности;

-недостаточно строгая аутентификация пользователей;

-отсутствие контроля доступа, нет возможности определить кто именно работает, к устройству так же имеет доступ окружение пользователя;

-возможна утечка информации с конечных устройств, даже при контроле копирования на внешние носители, например путем фотографирования информации с экрана.

Для минимизации возникновения предпосылок утечки конфиденциальной информации налоговых органов в режиме дистанционной работы сотрудников предлагаю следующие пути решения:

-рассматривать вопрос целесообразности перевода, возможно делегировать обязанности на другого сотрудника находящегося на службе;

-путем предоставления усеченных прав к информационным ресурсам на период дистанционной работы;

-ведение фото фиксации пользователя в рабочее время посредством веб-камеры установленной на конечном устройстве;

-установка специализированного ПО на конечном устройстве для контроля действий пользователя.

Таким образом, при дистанционной работе пользователь находится в ненадежной и неконтролируемой среде, в связи с чем, возникают предпосылки для утечки конфиденциальной информации налоговых органов.

ЗАКЛЮЧЕНИЕ

Теоретический анализ литературы по исследуемой в квалификационной работе проблеме позволил сделать следующие выводы:

Конфиденциальная информация - это информация, доступ к которой имеет ограниченный круг лиц, не подлежащая как предоставлению - передаче определенному кругу лиц, так и распространению - передаче неопределенному кругу лиц. Любая несанкционированная передача конфиденциальной информации нарушает установленный режим конфиденциальности и снижает ценность такой информации (значимой в силу неизвестности ее третьим лицам). Распространенная конфиденциальная информация полностью теряет свою ценность как объект права для ее обладателя. Предоставленная третьим лицам информация теряет часть такой ценности. Общество как обладатель информации не заинтересовано ни в первом, ни во втором.

Допуск должностных лиц и граждан к конфиденциальной информации осуществляет руководитель организации, учреждения, предприятия.

Правовой основой для допуска является:

- обязательство должностного лица (работника) о неразглашении сведений конфиденциального характера, закрепленное в трудовом договоре (контракте) согласно ТК РФ;

- нормативный правовой акт (документ) изданный или утвержденный руководителем организации определяющий порядок допуска и доступа к сведениям конфиденциального характера.

Для обеспечения правовой защищенности в полной мере служебной и коммерческой тайны "обязательство" (контракт) может составляться помимо трудового договора и содержать следующие обязательства работника:

- не разглашать сведения, составляющие служебную или коммерческую тайну организации, которые ему будут доверены или станут известны по работе;

- не передавать третьим лицам и не раскрывать публично сведения, составляющие служебную или коммерческую тайну организации без согласия администрации;

- выполнять требования приказов, инструкций и положений по обеспечению сохранности служебной и коммерческой тайны организации;

- в случае попытки посторонних лиц получить от него сведения о служебной или коммерческой тайне организации немедленно сообщить об этом руководителю структурного подразделения и начальнику службы

безопасности организации;

- сохранять служебную и коммерческую тайну тех предприятий, с которыми организация имеет деловые отношения;

- не использовать знания служебной или коммерческой организации для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб организации;

- в случае его увольнения все носители служебной или коммерческой тайны организации, которые находились в его распоряжении, передать организации;

- об утрате или недостаче носителей служебной и коммерческой тайны, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению служебной или коммерческой тайны организации, а также о причинах и условиях возможной утечки сведений, немедленно сообщить начальнику службы безопасности.

Кроме того, такое обязательство должно содержать последствия за нарушения указанных пунктов и применяемые меры со стороны администрации и со стороны органов судебной власти в соответствии с уголовным гражданским и административным законодательством.

Сотрудники организации должны руководствоваться порядком работы с документами, содержащими конфиденциальную информацию.

За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

По общему правилу степень защиты конфиденциальной информации должна соответствовать уровню ее ценности для обладателя. Перечень обязательных мер по охране конфиденциальности информации, принимаемых ее обладателем, в частности, включает: ограничение доступа к информации, составляющей тайну, путем установления порядка обращения с этой информацией и контроля за его соблюдением. Подчеркну, что обладатель информации должен принимать не только организационные и юридические меры к охране конфиденциальности информации, но и специальные технические, затрудняющие доступ третьих лиц к ней в компьютерной системе.

Таким образом, подводя итог вышеизложенному материалу можно сделать вывод, что главная задача защиты конфиденциальной информации - это защита доступа (физического или программного) к информации, содержащей сведения ограниченного доступа, так, чтобы максимально

обезопасить ее от несанкционированного доступа.

При работе с конфиденциальной информацией государственные и негосударственные структуры руководствуются нормативно-правовыми актами РФ, внутренними положениями о работе с документацией ограниченного доступа. Несоблюдение организации работы с конфиденциальной информацией может стать причиной её утечки.

БИБЛИОГРАФИЯ

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 28.06.2021, с изм. от 08.07.2021).

3. "Гражданский кодекс Российской Федерации (часть вторая)" от 26.01.1996 N 14-ФЗ (ред. от 09.03.2021, с изм. от 08.07.2021) (с изм. и доп., вступ. в силу с 29.06.2021).

4. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 01.07.2021).

5. "Налоговый кодекс Российской Федерации (часть первая)" от 31.07.1998 N 146-ФЗ (ред. от 02.07.2021).

6. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 11.06.2021) "Об электронной подписи".

7. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных".

8. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации".

9. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных".

10. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) "О коммерческой тайне".

11. Федеральный закон от 27.07.2004 N 79-ФЗ (ред. от 02.07.2021) "О государственной гражданской службе Российской Федерации".

12. Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 02.07.2021) "О техническом регулировании".

13. Закон РФ от 21.07.1993 N 5485-1 (ред. от 11.06.2021) "О государственной тайне".

14. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

15. Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации".

16. Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) "Об утверждении Перечня сведений, отнесенных к государственной тайне".

17. Приказ Федеральной налоговой службы от 06апреля 2021 г. № ЕД-7-24/298@ “О внесении изменений в Концепцию информационной безопасности Федеральной налоговой службы”.

18. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

19. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных".

20. Алексенцев А.И. Конфиденциальное делопроизводство. - М., 2018. 363 с.

21. Алексенцев А.И. Организация и технология размножения конфиденциальных документов / А.И. Алексенцев. 2019. № 4. 255 с.

22. Аникин И.В., Глова В.И., Нигматуллина А.Н. Методы и средства защиты компьютерной информации: Учебное пособие.Казань: КГТУ 2018.320 с.

23. Амелин Р. В. Информационная безопасность. М.: Юристъ, 2019. 121 с.

24. Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. 2017. № 4. 115 с.

25. Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореферат дис. канд. юрид. наук. - М., 2014.323 с.

26. Богдановская И.Ю. Право на доступ к информации. Доступ к открытой информации М.: ЗАО "Юстицинформ" 2019. 344 с.

27. Белова А.А. Соглашение о конфиденциальности в отечественном гражданском обороте // Вестник. 2019. № 1.201 с.

28. Беликов П.А. Новый метод управления жизненным циклом информации. Динамика ценности информации в базах данных // Труды IX Международной научно-технической конференции "Новые информационные технологии и системы". 2015.354 с.

29. Жилкина Т. Уничтожение электронных документов // Секретарское дело. 2016. № 10. 98 с.

30. Гришачев В. В. Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС // Специальная техника. 2019. № 2.107 с.

31. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А. Опасности возникновения каналов утечки конфиденциальной информации по волоконно-оптическим структурированным кабельным системам // Материалы X Международной научно-практической конференции "Информационная безопасность". 2018.214 с.

32. Данилов А.Д. Ценность информации // Технологии информационного общества. 2018. № 10. 198 с.

33. Дутов В. Предотвращение утечек информации // Управление рисками организации. 2018. № 3.154 с.

34. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. М.: ЮНИТИ-ДАНА. Закон и право 2017. 335 с.

35. Кучеров И.И. Налоговая тайна в системе мер защиты конфиденциальной информации / Налоговое право России: учебник / отв.ред. Ю.А. Крохина. - 6-е изд., испр. - М.: Норма, 2021. 403 с.