

УДК 346.9

Соколова Жанна Владимировна, к.и.н., доцент кафедры документоведения и архивоведения исторического факультета Таврической академии Крымского федерального университета имени В.И. Вернадского, г. Симферополь, Россия

e-mail: jcokol@mail.ru

Попова Анна Михайловна, обучающаяся юридического факультета Таврической академии Крымского федерального университета имени В.И. Вернадского

e-mail: poannmi@yandex.ru

ЗАКОНОДАТЕЛЬНАЯ И НОРМАТИВНАЯ РЕГЛАМЕНТАЦИЯ ДЕЛОПРОИЗВОДСТВА ОРГАНИЗАЦИИ

Аннотация. Для улучшения управляемости в организациях необходим процесс модернизации и автоматизации делопроизводства. Совершенствование методов управления документацией в современных условиях позволит целенаправленно формировать информационные ресурсы организаций, обеспечивать их эффективное функционирование, а также предоставлять доступ потребителям к информационным ресурсам с наименьшими затратами времени и сохранностью защиты информации.

Ключевые слова: концепция документооборота, регистрационная информация, формирование документа. юрисдикционный и неюрисдикционный порядок защиты информации, угрозы разглашения информации.

Sokolova J.V., Ph. D. in History, associate professor, Chair of Scientific Discipline of Documentation and Archival Science, History Department, Taurida Academy, V.I. Vernadsky Crimean Federal University, Simferopol, Russia

e-mail: jcokol@mail.ru

Popova A.M., student, Law Department, Taurida Academy, V.I. Vernadsky
Crimean Federal University, Simferopol, Russia
e-mail: poannmi@yandex.ru

LEGISLATIVE AND REGULATORY CONTROLS OF THE ORGANIZATION'S BUSINESS ADMINISTRATION

Annotation. A modernization and office automation process is essential to improve manageability in organizations. Improving the methods of document management in modern conditions will make it possible to purposefully form the information resources of organizations, ensure their effective functioning, as well as provide consumers with access to information resources with the least waste of time and the safety of information protection.

Keywords: documentation concept, login information, document formation, Jurisdictional and non-jurisdictional protection of information, threats of information disclosure.

Целью данной статьи является выявление, изучение и анализ проблем нормативно-правового регулирования сферы защиты информации в организации для ведения делопроизводства и выработки рекомендаций по ее совершенствованию, а также определение перспективных направлений развития теории и практики защиты информации в соответствии с государственными программами.

Порядок оформления, движения и хранения документов заключается в формировании условий, которые обеспечивают сохранности необходимой документации, ее отбор, организацию документооборота и обеспечение ею пользователей в поставленные сроки с минимальными расходами, исполнение и передача на архивное хранение.

Нормативная база регулируется: законодательными актами в сфере информации и документации; указами Президента, постановлениями

правительства, регламентирующих вопросы документационного обеспечения; правовыми актами органов исполнительной власти (министерств, комитетов, служб) как общепрофессионального, так и ведомственного характера; правовыми актами нормативного и инструктивного характера, методическими документами по делопроизводству организаций; государственными стандартами на ведение документации; нормативными документами по организации архивного хранения документов; унифицированными системами документации.

Документы, циркулирующих в организации, делятся на две большие группы:

- Документы по общим административным вопросам и вопросам общего руководства организацией.
- Документы по функциям управления (финансовых органов и функциональных подразделений).

Разработка разумной концепции документооборота совершается на ранних стадиях формирования компании. В период развития аппарата управления прямые обязанности распределяются между руководителями, обуславливается очередность согласования, подписания, установления и рассмотрения (разрешения) ключевых документов.

Действующие нормативные акты, в том числе и «Государственная концепция документационного обеспечения управления. Главные положения. Единые условия к документам и службам документационного обеспечения» (ГСДОУ), исходя из прагматических суждений, рассматривают в качестве предмета регулирования только лишь как документооборот организации в целом и поэтому потоки входящих, внутренних и исходящих документов формируются самостоятельно, исходя из необходимости самой организации.

В связи с возрастающими объемами обрабатываемых данных, накоплением и хранением данных в ограниченных местах, постоянным расширением круга пользователей, имеющих доступ информационным ресурсам, программам, а также недостаточный уровень защиты аппаратных и

программных средств компьютеров и коммуникационных систем, защита информации в современном мире приобретает исключительно важное значение.

Несмотря на серьезные положительные трансформации в сфере цифровизации – процесса постоянного измерения техническими средствами показателей работы специалистов или оборудования с целью сделать процесс работы наблюдаемым, управляемым и предсказуемым, все еще существует ряд актуальных и значимых нерешенных отраслевых проблем. Главным драйвером активизации такого процесса стало утверждение в июле 2017 г. Правительством Российской Федерации Программы «Цифровая экономика Российской Федерации». Согласно этой программе объектом защиты данных является информация, носитель информации или информационный процесс, который должен быть защищен. В соответствии с Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» сформирована национальная программа «Цифровая экономика Российской Федерации».

2 марта 2019 года Правительство РФ приняло Постановление N 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». В феврале 2019 года Президентом РФ утвержден Перечень поручений по вопросам реализации национальной программы «Цифровая экономика Российской Федерации».

Следовательно, объектом правовых отношений в информационной сфере является информация в разнообразных материализованных формах, то есть информация, которая находится в гражданском, административном или ином публичном обращении и в зависимости от того, какие социальные отношения возникают, подлежит правовому регулированию.

Предметом и объектом правовых отношений является нормативно-правовое регулирование информации, которое возникает при осуществлении информационных процессов, то есть процессов производства, сбора, обработки,

накопления, хранения, поиска и передачи информации.

Не стоит забывать, что современная практика обеспечения документационных процессов находится на стадии совершенствования и не удовлетворяет современным требованиям. Основной целью защиты информации является предотвращение утечек, хищения, что приводит к значительным потерям, но и подделка информации. Необходимо принять все меры по предотвращению несанкционированных действий, путем обеспечения блокирования. Это повысит уровень защиты информации от модификации, копирования и уничтожения. Значимой в сфере защиты информации является реализация права на государственную тайну и конфиденциальную информацию.

Таким образом, мы можем проследить тенденцию к тому, что роль права как основного механизма регулирования социальных отношений в информационном обществе резко возрастает. Процессы управления в социальных системах становятся приоритетными. Формирование информации тесно связано с формированием информационного права и с формированием информационного общества.

Главными угрозами информации являются:

- Утечка. В результате распространения защищенная информация не контролируется и не распространяется, формируется несанкционированный доступ к информации, и защищенная информация может быть получена с помощью разведки;

- Несанкционированное воздействие. Воздействие, приводящее к нарушению установленных прав или правил изменения информации, последствия чего приводят информацию к искажению, происходит блокирование доступа к ней. Это способствует сбою функционирования, а также уничтожению самого носителя информации;

- Непреднамеренное воздействие. Воздействие, приводящее к сбою функционирования носителя информации из-за ряда опасных угроз таких как уничтожение, копирование, искажение, а также блокировка данных. Эти угрозы

непреднамеренно имеют воздействие на изменение информации, что влечет за собой сбой всей программы документирования

- Разглашение. Информация не санкционировано доводится до потребителей, не имеющих права доступа к этой информации.

- Несанкционированный доступ. Происходит получение заинтересованным субъектом защищаемой информации, что является нарушением информационных прав собственника, которые зафиксированы в правовых документах, где обозначены правила доступа к ней.

Считаем, что для всех объектов правоотношений порядок защиты информации будет одинаковый, различают только юрисдикционный и неюрисдикционный порядки защиты.

Юрисдикционный порядок защиты – это деятельность государственного органа, которая способствует восстановлению права и пресечению действий, которые нарушают право. Юрисдикционный порядок делится, в свою очередь, на судебный и административный.

Неюрисдикционный порядок охватывает собой действия граждан и организаций по защите гражданских прав и охраняемых законом интересов, то есть это является некой самозащитой, которая совершается ими самостоятельно и без помощи компетентных органов. Обладатель оспариваемого или нарушенного права может использовать разнообразные способы по его защите. Это указано в ст. 12 ГК, где указанные действия объединены в понятие «самозащита гражданских прав» и рассматриваются в качестве одного из способов защиты гражданских прав.

Главными организационно-техническими мероприятиями, которые проводятся общегосударственной концепцией защиты информации, являются в области защиты информации:

1. Проведение государственного лицензирования работы учреждений и организаций;

Под лицензией понимается разрешение, которое дает право на виды работ в области защиты информации. Получение лицензии возможно при

условии, что организация имеет соответствующую производственную базу, ведет нормативно-методическую работу.

2. Проведение аттестации должно производиться в соответствии с требованиями информационной безопасности. Главное предназначение аттестации — это оценка готовности систем, а также средств информатизации вследствие обработки информации, которая содержит в себе государственные, служебные или коммерческие тайны.

3. Сертификация. Процедура сертификации систем защиты информации - это подтверждение соответствия установленным требованиям государственных стандартов или соответствию другим нормативным документам по защите информации.

4. Категорирование предприятий, выделенных помещений и объектов вычислительной техники по степени важности обрабатываемой информации.

5. Введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах эксплуатации технических средств, подлежащих защите;

6. Создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

7. Мероприятия по разработке и внедрению инновационных технических решений информационной защиты. Актуально для военной отрасли и систем связи.

Сформированный подход к классификации информации позволяет сделать вывод, что информация, защищенная в первую очередь, классифицируется как государственная информация. Данный подход классифицируется по уровню требований безопасности на основе одного из его свойств. Это свойство конфиденциальности, то есть секретности.

Следует выделить категории конфиденциальности:

Строго конфиденциальная. Под видом понимается информация, являющаяся конфиденциальной в соответствии с нормами функционирующего законодательства, а также информация, на распространение которой введены

определенные ограничения (коммерческая тайна) или распространение которой является тяжкими экономическими последствиями для организаций.

Конфиденциальная. Под видом понимается информация, которая в первую очередь не относится к категории «строго конфиденциальная». При разглашении данной информации возможна потеря конкурентоспособности организации, что в свою очередь сопровождается еще рядом факторов: нанесению ощутимого ущерба интересам клиентов, корреспондентов, партнеров или сотрудников.

Открытая. Под видом понимается информация, для которой нет необходимых ограничений

Порядок перемещения документов в учреждении представляется не таким важным по отношению к структуре учреждения и внутреннему распределению прямых обязанностей, в том числе неофициальную концепцию подчиненных взаимоотношений. Тем не менее, это не значит, что концепция учреждения рабочего процесса никак не поддается независимому регулированию и нормированию. ГСДОУ нуждается в укреплении порядка, связанного с перемещением документов внутри. Укрепление порядка происходит при поддержке службы делопроизводства и ратифицируемых начальством учреждений. Данные схемы должны содержать пункты, задачами которых будет обработка данных. Регулирующая функция вступает в силу только после утверждения начальством методики перемещения бумаг.

Обработка документов реализуется в течение 24 часов с момента появления в компании. Все движения и переводы оформленных документов должны фиксироваться и регистрироваться в журналах. Руководителем учреждения определяется порядок передачи данной информации. При подаче важного документа руководителю с целью подписания ему необходимо добавить материалы, на базе которых он был подготовлен.

На все поступающие документы должен быть установлен регистрационный штамп, например, на номер заказа квитанции, дату получения и, при надобности, число листов. На первой странице в нижнем правом углу

арабскими цифрами формируется регистрационная информация. Нумерация писем, телеграмм, факсов осуществляется в течение года, телеграмм с огромным их количеством - в течение месяца.

За подлинность сведений, содержащихся в документах, обязательство за выполнение графика документооборота, за уместное и высококачественное формирование документов, их своевременную передачу с целью отражения в бухгалтерском учете и отчетности, несут лица, кто создал и кто подписал эти документы.

Таким образом, решение проблемы управления документацией в современных условиях позволит целенаправленно формировать информационные ресурсы организаций, обеспечивать их эффективное функционирование, а также открывать доступ потребителей к информационным ресурсам с наименьшими затратами времени, труда и ресурсов с сохранением коммерческой тайны и неразглашением конфиденциальной информации.

Список литературы:

1. Басаков, М. И. Документационное обеспечение управления: (Делопроизводство) / М. И. Басаков. – 2-е изд., исп. и доп. – Ростов-на-Дону: Феникс, 2013. – 352 с.
2. Кузнецов, И. Н. Делопроизводство: учебное пособие: [16+] / И. Н. Кузнецов. – 9-е изд., перераб. – Москва: Дашков и К°, 2020. – 406 с.: ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=572967> (дата обращения: 01.10.2021). – Библиогр.: с. 312-323. – ISBN 978-5-394-03881-5. – Текст: электронный.
3. Рогожин, М. Ю. Организация делопроизводства предприятия: (на основе ГОСТ Р 6.30-2003) / М. Ю. Рогожин. – Москва; Берлин: Директ-Медиа, 2014. – 209 с.: ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253709> (дата обращения: 01.10.2021).

17.10.2021). – Библиогр. в кн. – ISBN 978-5-4458-6535-3. – DOI 10.23681/253709. – Текст: электронный.