ции и упростить процесс получения и обработки информации. Вместо того, чтобы нанимать специальных сотрудников для работы с бумажными документами и их архивацией, организации могут использовать электронные форматы документов и автоматизированные системы для их обработки и хранения. Это позволяет сократить ошибки, связанные с человеческим фактором, и повысить продуктивность работы. Также сотрудники при распределении своего времени меньше тратят его на подготовительные работы с документами, происходит более быстрая обработка информации, и поэтому они больше времени могут уделять другим видам деятельности.

Список источников и литературы:

Ланская Д. В., Арефьева И. В. Анализ преимуществ и проблем внедрения системы электронного документооборота в организацию // Деловой вестник предпринимателя. 2020. № 1 (1). 48–54.

Ларин М. В., Рысков О. И. Электронные документы в управлении: научно-методическое пособие. 2-е изд., доп. М.: ИПО «У Никитских ворот», 2008. 207 с.

Лебедева А. А. Сущностная характеристика понятия «тайм-менеджмент» // Молодой ученый. 2020. № 46 (336). С. 96–99. URL: https://moluch.ru/archive/336/75002/ (дата обращения: 26.03.2024).

Тайм-менеджмент: что это, как научиться управлять своим временем, обзор книг и приложений // Units. Платформа по быстрому освоению навыков. https://units.bz/media/taym-menedzhment-chto-eto-kak-nauchitsya-upravlyat-svoim-vremenem-obzor-knig-i-prilozheniy(дата обращения: 26.03.2024).

Хургин В. А. Еще раз об электронном документе // Информационные ресурсы России. 2008. № 3. С. 13–21.

УДК 005.922.1:004.63

Е. С. Прокофьева

Уральский федеральный университет

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Аннотация. Сегодня обеспечение надежной защиты информации является одним из ключевых вопросов национальной безопас-

ности России. В данной статье рассмотрим значимость безопасности электронного документооборота. Правовое регулирование защищённого электронного документооборота.

Ключевые слова: системы электронного документооборота, конфиденциальность информации, конфиденциальная документация, конфиденциальное делопроизводство.

В настоящее время проблема обеспечения безопасности конфиденциальных документов становится все более актуальной, поскольку технологии развиваются, а угрозы нарушения информационной безопасности становятся все более масштабными.

Количество утечек сведений ограниченного доступа в России и мире растёт, причем утечки конфиденциальной информации являются одной из основных угроз. Согласно данным ГК «СОЛАР» — одного из крупнейших игроков на российском рынке комплексных систем кибербезопасности, в первом полугодии 2023 г. было зафиксировано «1607 случаев успешных кибератак в мире, и в 59% этих инцидентов последствиями стали утечки конфиденциальной информации, в то время как за аналогичный период прошлого года зафиксировано 1416 инцидентов, в 42% из которых были утечки конфиденциальной информации» [Плата за утечку...].

Размещение даже 5% конфиденциальных данных в открытом доступе достаточно, чтобы компания утратила лидирующие позиции на рынке. Репутационные потери не поддаются прогнозированию и тесно связаны с финансовыми, т.к. оказывают прямое воздействие на снижение доходов из-за негативного восприятия компании [ГК «Солар»...].

Поэтому крайне важно обеспечить защиту конфиденциальных данных от несанкционированного доступа. Это включает в себя комплекс мер, направленных на контроль прав доступа пользователей. В организациях и на предприятиях вводятся ограничения на использование информации, которая не является необходимой для выполнения прямых рабочих обязанностей.

Защита электронного документооборота в настоящее время становится объектом внимания государства. Частные и государственные компании активно стремятся к развитию и внедрению в работу систем электронного документооборота:

— происходит развитие государственных услуг в электронном виде, в которых активно участвуют государственные служащие, в связи с чем возникают вопросы о защите конфиденциальной информации;

— услуги, которые предоставляются в электронном виде, должны базироваться в правовом поле. Как правило, в этом случае соз-

данию электронного документа предшествует огромная работа по обмену данными между различными ведомствами, а этот процесс не должен быть общедоступным, так как может содержать конфиденциальную информацию;

— появляется реальная необходимость сделать электронные документы юридически значимыми.

По этим причинам вопрос защиты электронного документооборота начинает рассматриваться на государственном уровне.

Таким образом, повышается актуальность поиска решений, которые будут направлены на обеспечение защиты конфиденциальной информации, что приводит к такому тренду, как внедрение в системы электронного документооборота механизмов автоматизации работы с электронными документами конфиденциального характера.

Эффективное обеспечение безопасности электронного документооборота требует комплексного подхода, включающего различные меры по защите информации и обеспечению конфиденциальности. Для достижения этой цели необходимо правильно организовать технические, программные и организационные мероприятия, направленные на ограничение доступа к конфиденциальной информации. Однако не стоит забывать о важной роли, которую играют сотрудники. Каждый из них должен осознавать свою ответственность за выполнение своих обязанностей в рамках безопасного документооборота.

Соблюдение законодательства и нормативных требований также играет роль в обеспечении безопасности конфиденциальной информации. Значительный объем документов конфиденциального характера, встречающийся в деятельности современных организаций, особенно сотрудничающих с заказчиками из госсектора, составляют документы для служебного пользования. Помимо Концепции национальной безопасности РФ [ФЗ № 400 от 02.07.2021], в которой приведены задачи обеспечения национальной безопасности в информационной сфере, рассмотрим ключевые нормативно-правовые акты, которые регулируют работу с документами для служебного пользования в рамках системы электронного документооборота:

1. Совместный приказ Минцифры России № 667 и ФСО России № 233 от 4 декабря 2020 г. «Об утверждении требований к организационно-техническому взаимодействию государственных органов и государственных организаций» [Приказ Минцифры России № 667 и ФСО России № 233 от 04.12.2020]. Его положения устанавливают, в каком формате должны производиться обмен и обработка документов по МЭДО 2.7.1. Правила в равной мере распространяются на документы «Для служебного пользования», для которых не предусмотрено каких-либо исключений.

2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», который говорит о необходимости аттестации узлов подключения МЭДО [Приказ ФСТЭК России № 17 от 11.02.2013].

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, а также применении информационных технологий и обеспечение защиты информации [ФЗ № 149-ФЗ от 27.06.2006].

4. Постановление Правительства РФ от 3 ноября 1994 г. № 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» [Постановление Правительства РФ № 1233 от 03.11.1994].

Что касается последнего постановления, то основная сложность заключается в том, что до сих пор не существует процедуры работы с конфиденциальными документами в электронном виде. Действующие правила распространяются на работы с информацией ограниченного доступа в бумажном виде. В ближайшем будущем ИТ-индустрия и государственные органы ожидают введения правил, специфичных для электронных конфиденциальных документов. А до тех пор заказчики и интеграторы дополняют свои системы электронного документооборота решениями, позволяющими максимально соответствовать требованиям действующих нормативных актов по работе с конфиденциальной информацией при переводе её в электронный формат.

Таким образом, с учетом существующих угроз для защиты национальных интересов России, государство уделяет особое внимание развитию отечественных индустрий в сфере информации, коммуникации и связи. Ключевым направлением является обеспечение гарантий безопасности для национальных информационных и телекоммуникационных систем. Для этого государство планирует внедрять передовые технические средства, разрабатывать и совершенствовать системы защиты информации, противодействовать кибератакам и несанкционированному доступу к данным. Особое внимание уделяется защите государственных секретов и конфиденциальной информации.

Список источников и литературы:

ГК «Солар»: Средний ущерб от одной утечки информации составил 5,5 млн. рублей // Администрация Сысертского городского округа. URL: https://admsysert.ru/info/actual/6667 (дата обращения: 28.01.2024).

О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ № 400 от 02.07.2021 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 14.02.2024).

Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27.06.2006 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 14.02.2024).

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: постановление Правительства РФ № 1233 от 03.11.1994 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_54870 (дата обращения: 14.02.2024).

Об утверждении требований к организационно-техническому взаимодействию государственных органов и государственных организаций: совместный приказ Минцифры России № 667 и ФСО России № 233 от 04.12.2020 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_378897 (дата обращения: 14.02.2024).

Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России № 17 от 11.02.2013 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_147084 (дата обращения: 14.02.2024).

Плата за утечку. ГК «Солар» посчитала, сколько бизнес потерял на краже данных // iTrend. URL: https://itrend.ru/news/Plata-za-utechku.-GK-Solar-poschitala-skolko-biznes-poteryal-na-krazhe-dannykh-5423 (дата обращения: 28.01.2024).

УДК 005.92:004.63:004.8

Е. Д. Редопупова[1]

Российский Государственный профессионально-педагогический университет

РОБОТИЗИРОВАННАЯ ДОКУМЕНТАЦИЯ И ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Актуальность данной темы обусловлена тем, что в эпоху пост индустриального общества и полной автоматизации

[1] Научный руководитель: М. Б. Ларионова, кандидат исторических наук, доцент РГППУ.