УДК 004.8

БЕЗОПАСНОСТЬ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Лях Е. А., Макеева А. С.

Южно-Российский институт управления – филиал РАНХиГС

e-mail: lyakhekaterina@mail.ru, al.makeeva.00@gmail.com

Аннотация: в данной статье приводится характеристика и обосновывается актуальность использования систем электронного документооборота. Анализируются угрозы информационной безопасности в системах электронного документооборота, приводятся направления повышения безопасности.

Ключевые слова: система электронного документооборота, СЭД, безопасность, информация, цифровизация.

SECURITY IN THE ELECTRONIC DOCUMENT MANAGEMENT SYSTEM

Lyakh E. A., Makeeva A. S.

Annotation: this article describes and substantiates the relevance of using electronic document management systems. The threats to information security in electronic document management systems are analyzed, and directions for improving security are given..

Keywords: electronic document management system, EDMS, security, information, digitalization.

Современный этап общественного развития обусловлен тем, что во всех развитых странах мира под влиянием процессов научно-технического прогресса значительно изменяются и совершенствуются процессы взаимодействия с информацией, поскольку именно информация несет в себе особую ценность.

Процесс распространения информации охарактеризован развитием систем документооборота, в том числе и электронного. Поскольку в современном мире, значительное количество процессов переходят в онлайн-режим, электронный документооборот приобретает особую важность и становится инструментом, обеспечивающим повышение эффективности деятельности.

О необходимости перехода от бумажного делопроизводства к системам электронного документооборота говорят уже давно, подчеркивая его основные преимущества, в частности такие как: мгновенный доступ к информации, повышение производительности организации, уменьшение издержек, минимизация влияния «человеческого фактора» и т.д.

СЭД выступает одним из фундаментальных элементов взаимодействия в процессе реализации задач между отделами, подразделениями, органами управления, контрагентами и т.д. Многие российские и зарубежные компании в своей деятельности подчеркивают, что внедрение систем электронного документооборота позволяет усовершенствовать процессы обмена информации, облегчить коммуникацию и ускорить взаимодействие. Так, на

сегодняшний день, более 90% отечественных компаний осуществляют свою деятельность с использованием современных системы электронного документооборота. Динамика роста в долевом выражении компании, использующих системы электронного документооборота в России, представлена на рисунке 1.

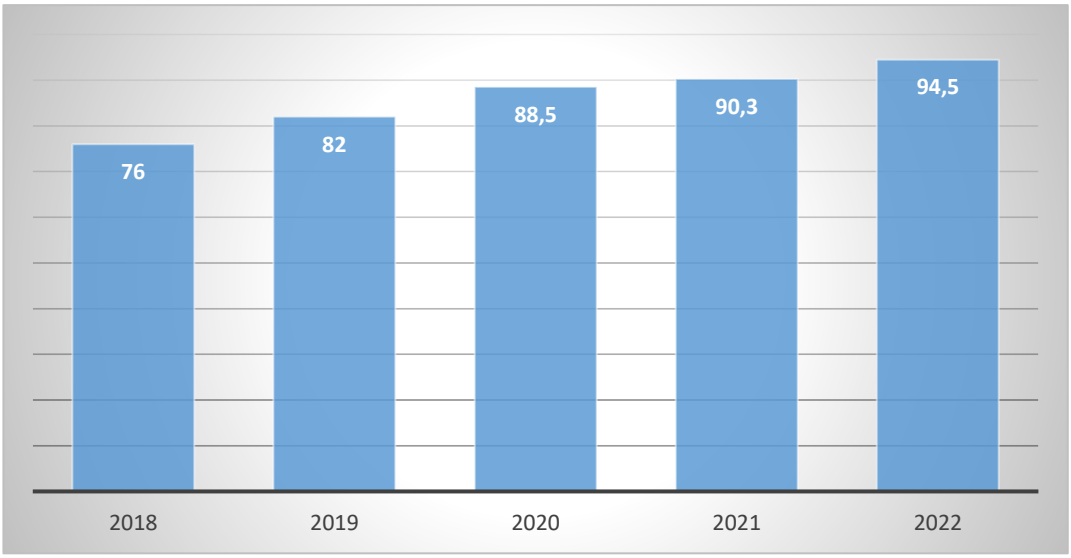

Рисунок 1. Динамика компаний в РФ, использующих электронный документооборот в %[1]

Но, хотелось бы отметить, что несмотря на всю совокупность преимуществ от внедрения СЭД, данный процесс обусловлен появлением новых рисков и угроз объектам информационной безопасности. Так, в прошлом году ведущей компанией в области информационной безопасности – InfoWatch было проведено исследование, в котором выявлено, что на территории Российской Федерации произошел резкий скачок количества утечки данных. Так, количество утечки информации увеличилось почти втрое в сравнении с 2017 годом и составило 710[2].

Рисунок 2. Количество утечек данный в России в период 2017-2022 гг. [2]

Полный переход на электронный документооборот неизбежен с позиции эволюции экономических систем и научно – технического прогресса, но следует учитывать все возникающие риски, формируя стратегии и программы развития цифровой среды на научной основе.

Вследствие этого, компании, использующие системы электронного документооборота, должны не только опираться на преимущества СЭД, но и обеспечить комплекс мероприятий, которые направлены на предупреждение и минимизацию последствий атак.

Комплекс мероприятий по обеспечению информационной безопасности СЭД должен опираться на нормы законодательства РФ. Так, положения Федерального закона№ 152-ФЗ «О персональных данных» [3] позволяет определить способы обработки, хранения и доступа к информации, совокупность прав субъекта персональных данных, обязанности операторов и меры ответственности. Согласно Федеральному закону № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (КИИ)[4], под его действие попадают не только государственные органы и учреждения, крупный бизнес, но и средние и небольшие компании, представленные как через юридические лица, так и индивидуальных предпринимателей.

Необходимость формирования комплексной нормативно-правовой базы по обеспечению информационной безопасности обусловлена тем фактом, что на сегодняшний день усложнились угрозы СЭД. В частности, в зависимости от классификационных характеристик угрозы могут быть естественными и искусственными, антропогенными и техногенными, стихийными и т.д.

Наиболее часто повреждение информации, а именно в 45% случаев, происходит в связи с физическими причинами, таким как стихийные бедствия, поломка аппаратуры и т.п. В 35% случаев угрозами для информационных данных выступают ошибки пользователя, а около 20% - обусловлено вредоносными программами и хакерскими атаками.

В качестве основных направлений повышения безопасности электронного документооборота следует выделить:

- преобразование файлов в специальный формат, что позволит обеспечить защиту от перехвата информации;
- привязка к устройству получателя, что позволит получать доступ к информации лишь на легитимном компьютере;
- контроль распространения и использования, который позволяет отслеживать открытие документов в режиме реального времени с учетом географических и временных характеристик.

Таким образом, можно сделать вывод, что для эффективного использования системы электронного документооборота следует обращать внимание не только на несомненные плюсы, но и на угрозы, которые обусловлены необходимостью обеспечения информационной безопасности. В деятельности организаций, которые применяют системы электронного документооборота должен применяться комплексный подход которые будет обеспечивать защиту информации на всех уровнях: от физической защиты до использования инновационных технологий и искусственного интеллекта.

Список литературы

1. Дупленко А. Г. Средства криптографической защиты электронного документооборота //Проблемы сертификации, управления качеством и документационного обеспечения управления. – 2022. – С. 25-28.
2. Белов И. И. Роль технологий искусственного интеллекта в цифровой трансформации делопроизводства и архивного дела // Научный вестник Крыма. 2022. №4 (39).
3. Утечки информации ограниченного доступа в России за 2022 год URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god (дата обращения 27.10.2023 г.)
4. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» // Российская газета от 29 июля 2006 г. N 165.
5. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» //Российская газета от 31 июля 2017 г. N 167.