Фомина П.С., Морозова М.Ю.
ЮРИУ РАНХиГС
Ростов-на-Дону
Научный руководитель:
К.пед.н., доц., Перова М.В.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация: *в данной работе проведен анализ использования различных методов обеспечения информационной безопасности в системах электронного документооборота.*

Ключевые слова: *информационная безопасность, электронный документооборот, блокчейн, цифровая экономика, искусственный интеллект.*

ENSURING INFORMATION SECURITY IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Annotation: *in this paper, the analysis of the use of digital technologies different support of information security in electronic document management systems is carried out.*

Keywords: *information security, electronic document management, blockchain, digital economy, artificial intelligence.*

Системы электронного документооборота (СЭД) в современном мире являются неотъемлемой частью функционирования любой организации, поскольку экономит время и ресурсы на обработку бумажной документации.

По данным аналитиков исследовательского центра «Контур» в начале 2023 года количество документов в системах электронного документооборота увеличилось на 35% с аналогичным периодом прошлого года. Эксперты объясняют положительную тенденцию тем, что происходит перевод бизнес-процессов в онлайн режим.

Усовершенствование СЭД стоит наравне с развитием обеспечения безопасности как с нормативно-правовой, так и цифровой точки зрения [1].

На основе исследований следующих авторов был проведен анализ методов информационной защиты систем электронного документооборота: Козлов А.А., Григорьева М.В., Шестаков О.В., Кузнецова Е.А.

Актуальность данной работы обусловлена тем, что со стремительным развитием технологий в использовании системы электронного документооборота, необходимо обеспечивать сохранение конфиденциальности документов при помощи нормативно-правовой базы, технических и организационных методов.

Эксперты выделяют следующие основные угрозы для процесса электронного документооборота:

1. Угроза конфиденциальности (изменение маршрутов обработки, кража данных);
2. Угроза целостности информации (повреждение или несанкционированное уничтожение информации);
3. Угроза доступности информации (сетевые атаки, вредоносное программное обеспечение).

Кроме того, существуют внутренние (злоумышленники, в лице действующих или бывших сотрудников организации, получившие доступ к СЭД) и внешние (злоумышленники, получившие несанкционированный доступ к СЭД) источники угроз.

По данным «1С-интегратор» не менее 70% потерь информации происходит в результате внутренних атак на систему электронного документооборота.

К методам информационной безопасности СЭД относят: технические, нормативно-правовые, организационные.

В России основным законодательным актом в области информационной безопасности является Федеральный закон Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», устанавливающий требования

к защите информации, включая электронную информацию, а также включающий определение ответственности за нарушение законодательного акта.

Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», определяющее требования к защите персональных данных при обработке в системах электронного документооборота.

Также помимо нормативных актов в Российской Федерации действуют государственные стандарты по информационной безопасности:

-ГОСТ Р 50922-2007 Защита информации. Термины и определения.

-ГОСТ Р 51275-2007 Защита информации. Объекты информатизации.

На основе законодательства существуют следующие технические методы информационной безопасности систем электронного документооборота:

1. Шифрование данных;
2. Цифровая подпись;
3. Аутентификация и управление доступом;
4. Межсетевой экран (ограничение доступа для неавторизированных пользователей);
5. Использование и своевременное обновление антивирусного программного обеспечения;
6. Обучение и регулярный инструктаж сотрудников об основах и методах безопасности СЭД.

В свою очередь организационные меры безопасности – это комбинации различных методов обеспечения информационной защиты. Отличительными чертами являются: комплексность, актуальность, постоянный контроль за системой электронного документооборота.

Кроме того, Федеральная служба по техническому и экспертному контролю является государственным органом, ответственным за обеспечение

информационной безопасности на территории Российской Федерации и выполнение процедур, таких как: сертификация программных продуктов, установление требований к защите информации, регулирование использования иностранных ПО, консультации и аудит в области информационной безопасности.

Аналитики InfoWatch провели исследование утечек информации на территории России из СЭД за прошлый год и выявили негативную тенденцию. Утечки информации в государственном и коммерческом секторе стали более массовыми как по количеству документов, так и по объему украденной информации.

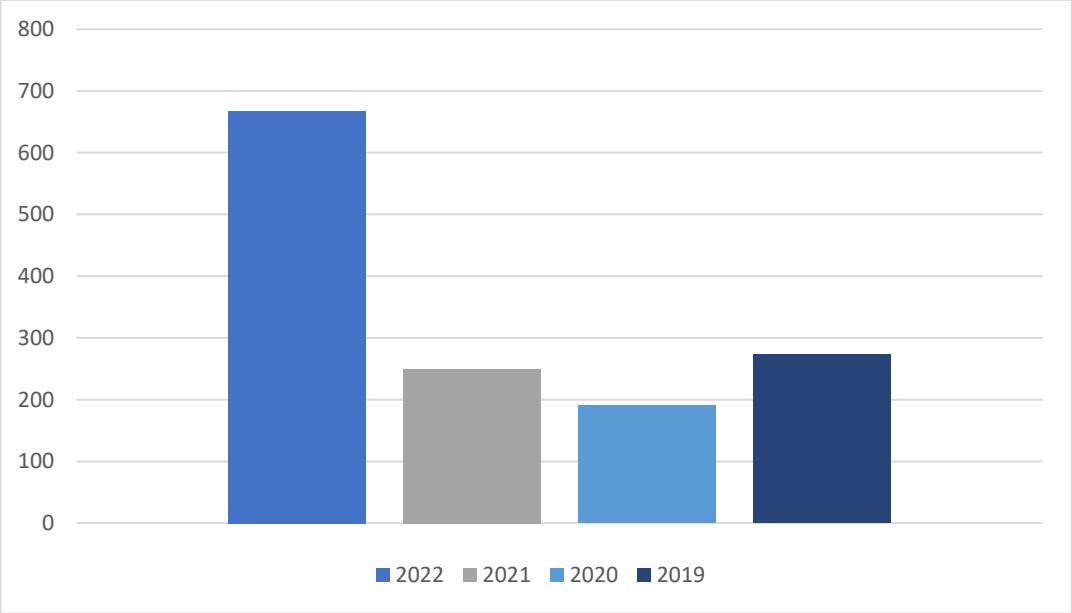

Рис.1 – количество взломанных данных СЭД

На данный момент основной проблемой в защите электронного документооборота является плохо проработанная система организационных методов безопасности. Каждая компания должна проанализировать: использует актуальные способы предостережения утечки конфиденциальной информации?

Для того, чтобы предотвратить утечку документации, организации должны следовать таким правилам:

1. Наличие юриста для защиты персональных данных в нормативно-правовой сфере;
2. Наличие штаба специалистов по it-технологиям для технических методов защиты СЭД;
3. Приобретение компанией новейшего программного обеспечения (антивирусы, форвейл, лицензионные программные продукты);
4. Постоянный инструктаж, тестирование и обучение сотрудников компании по использованию и информационной защите СЭД;
5. Разработка плана мероприятий по контролю и тестированию исправной работы СЭД.

По данным отчета Касперского за 2022 год основной удар злоумышленников пришелся на организации сферы «Ритейл» (27%). От 10 до 12% всех утечек произошли в организациях сфер «Карьера и образование», «Интернет-сервисы» и «Рестораны и доставка еды».

Наименьшему количеству взломов в 2022 году подверглись компании финансовой сферы, здравоохранения и недвижимости. Стоит отметить, что в перечисленных областях хранятся наиболее чувствительные пользовательские данные.

Рис.2 -количество утечек данных по отраслям

Таким образом, защита систем электронного документооборота требует разработки стратегий и политик безопасности, обучения персонала и постоянного мониторинга системы на наличие уязвимостей. Кроме того, необходимо соблюдать законодательные требования по защите персональных данных.

Библиографический список:

1. Козлов А.А., Григорьева М.В. Системы электронного документооборота: технологии и применение. М.: Издательство Юрайт, 2022;

2. Петров А.В., Кузнецова Е.А. Безопасность информации в системах электронного документооборота. М.: Издательство НИЦ ИНФРА-М, 2019;

3. Шестаков В.В, Шестамкова О.В. Безопасность информации в СЭД: проблемы и решения. М.: Издательство Форум, 2020.

4. Казаков А.В., Кузнецова Е.А. электронный документооборот в организациях: технологии и безопасность. М.: Издательство Юрайт, 2022.

5. Руководство по защите информации в системах электронного документооборота. М.: Издательство ФГУП «ГОСЭКАСПЕРТИЗА», 2019.