2. Интеллектуальная обработка текста [Электронный ресурс]. Официальный сайт компании «Digital Design». Режим доступа: <https://digdes.ru/nlab/intellektualnaya-obrabotka-tekstov> (дата обращения 10.11.2021).
3. Классификация данных при помощи нейронных сетей [Электронный ресурс]. Аналитическая платформа «Loginom». Режим доступа: <https://loginom.ru/blog/neural-classification> (дата обращения 10.11.2021).
4. Что такое нейронная сеть? [Электронный ресурс]. Официальный сайт компании «IDM». Режим доступа: <https://www.ibm.com/docs/ru/spss-statistics/SaaS?topic=networks-what-is-neural-network> (дата обращения 10.11.2021).
5. Составлено авторами на основе Конференции «Осенний документооборот – 2021» [Электронный ресурс]. Официальный сайт компании «EOS». Режим доступа: https://eos.ru/eos_calendar/eos_conf/2021.php (дата обращения 11.11.2021).
6. Указ Главы Республики Саха (Якутия) от 30.12.2018 № 312 (ред. от 05.02.2020) "О Единой системе электронного документооборота" [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/regbase/cgi/online.cgi?req=doc;base=RLAW249;n=77926#K6UsOoS2yTiNQSet> (дата обращения 11.11.2021).
7. Опыт использования нейросети для классификации документов в СЭД [Электронный ресурс]. Официальный сайт компании «EOS». Режим доступа: <https://eos.ru/upload/od2021/Neiroset.pdf> (дата обращения 11.11.2021).
8. Системы искусственного интеллекта — их развитие и области применения [Электронный ресурс]. Официальный сайт компании «Directum». Режим доступа: <https://www.directum.ru/blog-post/1927> (дата обращения 11.11.2021).

Перова М.В., Пономарев Д.А., Закладная А.В.
Безопасность электронного документооборота

*Южно-Российский институт управления филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации
(Россия, Ростов-на-Дону)*

doi: 10.18411/trnio-01-2022-50

Аннотация

В статье анализируются основные тенденции и проблемы обеспечения безопасности электронного документооборота в рамках цифровой трансформации, рассматривается нормативно-правовая регламентация данного процесса. Приводится анализ распространённых угроз информационной безопасности электронного документооборота.

Ключевые слова: информационная безопасность, уязвимости, обновления безопасности, социальная инженерия.

Abstract

This article analyzes the main trends and problems of ensuring the security of electronic document management in the context of digital transformation. It also examines the regulatory and legal regulation of this process and contains the analysis of common threats to the information security of electronic document management.

Keywords: IT Security, vulnerabilities, security updates, social engineering.

Вопрос о защите информации уже закреплён на официальном уровне. Об этом свидетельствует национальная программа «Цифровая экономика Российской Федерации», в рамках которой предусмотрено направление «Информационная безопасность» [1]. В масштабе данного направления особо выделяются угрозы, связанные с ростом компьютерной преступности, недостаточными разработкам отечественного программного обеспечения и низким качеством кадрового состава в области информационной безопасности [2]. Стратегия национальной безопасности РФ до 2030 года выделяет информационную безопасность как стратегически национальный приоритет [3].

В рамках электронного документооборота механизмы защиты от основных угроз приобретает все большее значение. И здесь Федеральная налоговая служба Российской Федерации (далее – ФНС) имеет большой опыт. В ФНС существует рабочая группа по разработке Концепции информационной безопасности при развитии электронного

документооборота в хозяйственной деятельности [4]. В Концепции определены меры и средства обеспечения защиты информации именно с привязкой к терминологии и к механизму электронного документооборота. В проекте текста Концепции сформированы основные рекомендации для операторов, разрабатывающих системы электронного документооборота, в том числе по учету требований, норм и принципов защиты информации на всех стадиях движения документа.

Вышеперечисленные данные позволят сделать заключение об актуальности исследуемой темы. Подробно раскрыть ключевые проблемы обеспечения информационной безопасности в системах электронного документооборота поможет наш последующий анализ.

Прежде чем приступить к анализу актуальных уязвимостей стоит отметить несколько тенденций электронного документооборота. Во-первых – переход на дистанционный формат работы ввиду пандемии вынуждает большинство компаний переходить с толстых клиентов систем электронного документооборота на соответствующие веб-приложения. Во-вторых – не стоит забывать, что для связи с субъектами вне систем электронного документооборота всё ещё используется электронная почта, которая является излюбленной точкой проникновения в системы при помощи социальной инженерии, которая, в свою очередь, всегда была и остаётся популярным инструментом киберпреступников.

Веб-приложения на данный момент являются наиболее уязвимыми системами, так как в секторе электронного документооборота они стали активно развиваться совсем недавно. Что касается социальной инженерии, то здесь стоит учесть, что 15% пользователей совершают потенциально опасные действия при получении фишинговых писем. Действительно, этот показатель стал намного ниже за последние годы, однако он недостаточно низок, чтобы не считать фишинг актуальной угрозой.

Рисунок 1. Статистика уязвимостей внешнего периметра

Давайте теперь проанализируем самые распространенные уязвимости внешнего (Рис. 1) и внутреннего периметра. Самая распространенная уязвимость внешнего периметра – это CVE-2015-0204. Данная уязвимость обнаружена в марте 2015 года в известном пакете свободно распространяемого ПО с открытыми исходными текстами под названием OpenSSL. Далее идет CVE-2015-4000 – компрометирующая TLS соединения, по своей природе схожа с предыдущей, то есть нацелена на веб-соединение. Стоит отметить уязвимость CVE-2020-0796, которая затрагивает протокол SMBv3. Данная уязвимость была обнаружена в марте 2020 года и является критической и актуальной, даже не смотря на патч от Microsoft.

Стоит обозначить важность обновлений. В 92% организаций отсутствует ручной или полу-ручной процесс обновления ПО. Более того, среднее время установки обновлений – 45 дней, в то время как злоумышленникам, при наличии навыков проникновения, будет достаточно 4 часов.

Таким образом можно отметить неэффективность одного из главных методов повышения уровня информационной безопасности – информирования. Обычные пользователи регулярно информируются о том, как важно соблюдать самые базовые правила информационной безопасности, однако, до сих пор в компаниях наблюдаются грубые нарушения информационной безопасности. Это означает, что советы не работают должным образом, так как фундаментальные угрозы до сих пор допускаются, притом не только рядовыми пользователями, но и сотрудниками информационной безопасности.

Возвращаясь к безопасности внешнего периметра, стоит отметить использование учетных данных по умолчанию. Это глобальная проблема в распространенных парольных политиках. Даже применяя требования на наличие символов верхнего, нижнего регистра, цифр и специальных символов, многие пароли всё ещё подбираются через брутфорс по словарям популярных комбинаций.

Теперь обратим внимание на внутренний периметр. В нём также актуально использование паролей по умолчанию, а также некорректное управление паролями. Множество систем, в которых работает электронный документооборот, уже снабжены средствами защиты, однако их наличие не означает полную безопасность – необходима корректная настройка.

Теперь обратимся к социотехническим исследованиям. Наименее успешным способом является вложенный docx-документ – только 1% пользователей совершили потенциально опасные действия. Однако письма со ссылками несут большую угрозу – 15% пользователей перешли на потенциально опасные веб-страницы, а 19% пользователей и вовсе ввели свои данные в подозрительные веб-формы.

Таким образом, мы убеждаемся в том, что безопасность электронного документооборота – всё ещё актуальная проблема, которая, несмотря на регулярные предупреждения специалистов, с каждым годом становится всё больше и больше. Организациям стоит обратить внимание на финансирование отделов информационной безопасности и регулярно проводить проверки квалификации сотрудников, чтобы не потерять контроль над собственным делопроизводством, что повлечет за собой огромные убытки.

1. Распоряжение Правительства Российской Федерации от 28.07.2017 №1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_221756/ (Дата обращения 11.11.2021).
2. «Информационная безопасность» [Электронный ресурс] // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. – Режим доступа: <https://digital.gov.ru/ru/activity/directions/874/> (Дата обращения 11.11.2021).
3. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_389271/ (Дата обращения 11.11.2021).
4. Распоряжение ФНС России от 13.11.2020 № 322@ (ред. От 11.04.2021) «О подгруппах по направлениям развития электронного документооборота с представителями бизнес-сообщества» [Электронный ресурс] // Официальный сайт Федеральной налоговой службы. – Режим доступа: https://www.nalog.gov.ru/rn77/related_activities/el_doc/el_bus_entities/10927823/ (Дата обращения 11.11.2021).