УДК 338.28

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Перова М.В., Пономарев Д.А.

Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Ростов-на-Дону, e-mail: perova_mv@uriu.ranepa.ru

В статье исследуются основные направления и пути решения проблем обеспечения информационной безопасности в современных системах электронного документооборота в контексте цифрового развития РФ, рассматривается нормативно-правовая регламентация данного процесса. Целью данного исследования является подробный анализ аспекта безопасности в условиях цифровой трансформации экономической системы Российской Федерации и изучение информационной безопасности электронного документооборота как необходимого компонента целостности экономических процессов при взаимодействии частного сектора и государственных учреждений при реализации цифровой экономики. Приводится анализ распространённых угроз информационной безопасности электронного документооборота, а также вопрос перехода на отечественные системы электронного документооборота в соответствии с политикой импортозамещения и установления цифрового суверенитета. Основным методом данного исследования является изучение отчетов аналитических компаний, специализирующихся на оказании услуг в сфере кибербезопасности как в частном, так и государственном секторах, а также изучение нормативно-правовой базы информационной безопасности электронного документооборота на территории Российской Федерации. Результатом данного исследования является выявление проблемных зон в области информационной безопасности организаций и задач, требующих внимания специалистов данной сферы деятельности.

Ключевые слова: информационная безопасность, уязвимости, социальная инженерия, импортозамещение, утечки

ENSURING INFORMATION SECURITY IN SYSTEMS OF ELECTRONIC DOCUMENT MANAGEMENT

Perova M.V., Ponomarev D.A.

Southern Russian Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration, Rostov-on-Don, e-mail: perova_mv@uriu.ranepa.ru

This article researches the main trends and problems solutions of ensuring the security in modern systems of electronic document management in the context of digital development of Russia. The purpose of this study is a detailed analysis of security aspect in the conditions of digital transformation of economic system in Russian Federation and study of information security of electronic document management as a necessary component of the integrity of economic processes in the interaction of the private sector and government agencies in the implementation of the digital economy. 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, as well as the issue of switching to domestic electronic document management systems in accordance with the import substitution policy and establishment of digital sovereignty. The main method of this research is the study of reports of analytical companies specializing in the provision of services in the field of cybersecurity in both private and public sectors, as well as the study of the regulatory framework for information security of electronic document management on the territory of the Russian Federation. The result of this study is the identification of problem areas in the field of information security in organizations, and what should be paid attention to by specialists in this field of activity.

Keywords: IT Security, vulnerabilities, social engineering, import substitution, leaks

В современной экономической системе Российской Федерации идёт активная трансформация практически всех направлений и осуществляется переход на новую модель цифровой экономики. Такое масштабное и комплексное изменение всех экономических и политических процессов ведёт к фундаментальным переменам, а это значит, что в новых реалиях потребуются новые средства безопасности, и в случае цифрового пространства – информационная безопасность. Данная область в сфере экономики и народного хозяйства ставит целый ряд особых задач, таких как обеспечение цифрового суверенитета, минимизация рисков при ведении деятельности в цифровом пространстве как частных организаций, так и государственных учреждений, а также сохранение целостности всей экономической системы с учётом новых информационных угроз, которые стали как никогда актуальны в контексте всеобщей цифровизации.

Огромную роль в экономическом взаимодействии частного и государственного сектора играют системы документооборота, которые также совершенствуются и адаптируются под цифровое пространство, что приводит к появлению новых, современных платформ электронного документооборота (ЭДО). Данная сфера так-

же нуждается в обеспечении безопасности в целях обеспечения стабильного и эффективного функционирования организации, что делает данную задачу весьма актуальной. Вопросы обеспечения информационной безопасности систем ЭДО рассматривались в работах ряда исследователей: Мирошниченко М.А., Бондаранко А.А., Пиналова Е.В., Евдокимова Л.М., Корябкин В.В. и др. [1-2]. Однако на данный момент актуализируется процесс разработки новых, а также дополнение существующих направлений, например разработка регламентационных баз, которые посредством федеральных органов власти будут эффективно регулировать политику информационной безопасности в экономическом секторе, где особую роль играет цифровой суверенитет, призванный минимизировать импортные технологические риски. Более того, электронный документооборот также является важным управленческим механизмом, защитой которого занимаются как государственные службы (ФСБ, ФСТЭК, ФСО), контролирующие на основе официальной регламентации исполнение всех мер информационной безопасности, так и частные компании, специализирующиеся на оказании услуг в области кибербезопасности.

Цель исследования: анализ аспектов информационной безопасности в условиях цифровой трансформации экономической системы Российской Федерации и определение направлений, способствующих обеспечению безопасности в системах электронного документооборота как необходимого компонента целостности экономических процессов при информационном взаимодействии частного сектора и государственных учреждений в процессе реализации цифровой экономики.

Материал и методы исследования

Информационная основа исследования – официальные данные, представленные: экспертами компании Positive Technologies, специализирующейся на разработке инновационных решений в сфере информационной безопасности; российской компанией InfoWatch, занимающейся защитой корпораций от утечек информации и целевых атак извне, а также центром противодействия кибератакам Solar JSOC; отделом технических расследований Solar JSOC CERT. В исследовании используется опыт Федеральной налоговой службы Российской Федерации (ФНС), в частности результаты работы рабочей группы по разработке Концепции информационной безопасности при развитии электронного документооборота в хозяйственной деятельности, а также регламентирующие документы ФСБ, ФСТЭК, ФСО.

Использованные методы исследования: методы статистической обработки данных, метод научной абстракции, методы индукции и дедукции. Исследование базируется на общих методах научного анализа, включая систематизацию, обобщение, абстрагирование, аналогию, анализ и синтез, опирается на понятийный аппарат, используемый современной наукой в контексте таких категорий, как экономика, управление, цифровая трансформация, информационная безопасность, эффективность, информационные технологии, системы эффективного электронного взаимодействия в контексте развития систем электронного документооборота и другие.

Результаты исследования и их обсуждение

Изучая актуальные киберугрозы третьего квартала 2021 года, представленные экспертами компании Positive Technologies, можно выделить следующие категории жертв среди организаций, которые наиболее часто подвергаются кибератакам (рис. 1).

Анализируя представленные данные, можно заметить, что государственные учреждения в 21% случаев являются основной целью киберпреступников. Однако именно в данной сфере огромную роль играют системы электронного документооборота (СЭД), что ещё раз подчеркивает важность обеспечения информационной безопасности, ведь именно ЭДО чаще других подвергаются атакам, в то время как данные системы содержат конфиденциальную, секретную или иную ценную информацию управленческого характера.

Данная проблема является актуальной, и многие респектабельные источники, такие как вышеуказанные Positive Technologies, а также InfoWatch, центр противодействия кибератакам Solar JSOC; отдел технических расследований Solar JSOC CERT – занимаются подробными исследованиями в сфере информационной безопасности. Данные этих исследований также применимы и к системам электронного документооборота. В рамках данного исследования мы проанализируем эти данные и выясним, в каком направлении необходимо работать как частным компаниям, так и государственным учреждениям. Таким образом, цель данного исследования – изучение актуальных проблем в сфере информационной безопасности электронного документооборота и определение того, какие пути решения уже существуют, а какие стоит разработать с учетом данных вышеописанных исследователей.

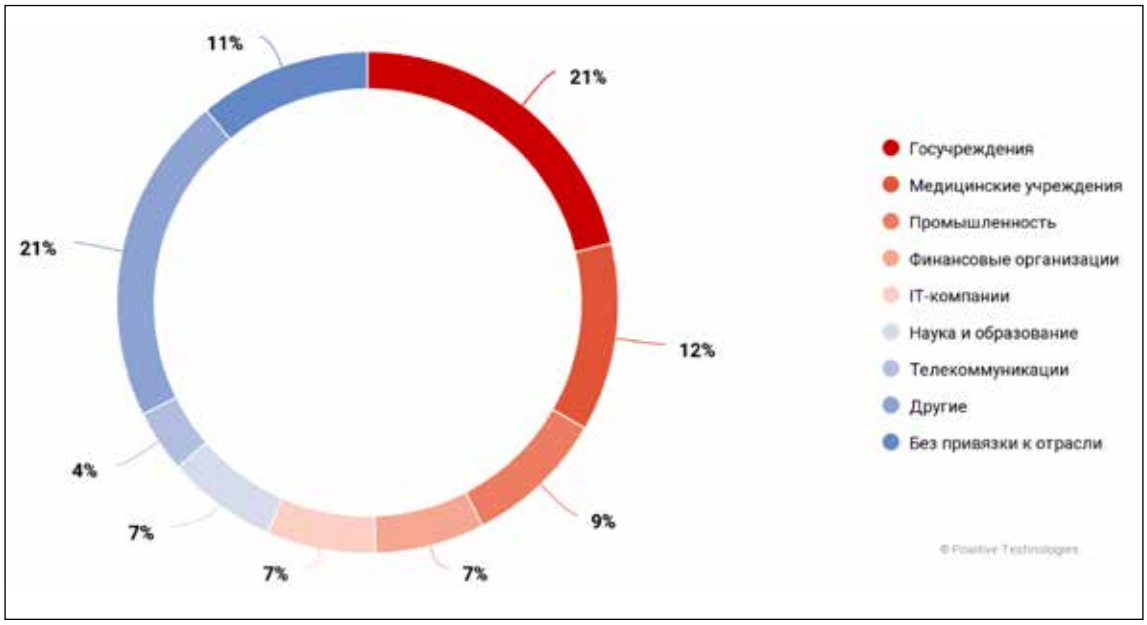

Рис. 1. Категории жертв среди организаций [3]

С точки зрения современных методологий управления – документ является главным источником управленческой информации. С переходом на системы электронного взаимодействия, с помощью которых обрабатывается огромное количество информации, в том числе конфиденциального характера, вопрос о безопасности становится одним из важных элементов исследования в рамках развития современного делопроизводства. На сегодняшний день, когда мы говорим о цифровой трансформации и переходе к цифровой экономике, необходимо понимать, что без информационной безопасности она не сможет эффективно функционировать, постоянно подвергаясь рискам.

Вопрос о защите информации уже закреплён на официальном уровне. Об этом свидетельствует национальная программа «Цифровая экономика Российской Федерации», в рамках которой предусмотрена реализация федерального проекта «Информационная безопасность» [4]. В масштабе данного направления особо выделяются угрозы, связанные с ростом компьютерной преступности, недостаточными разработками отечественного программного обеспечения и низким качеством кадрового состава в области информационной безопасности [5]. Стратегия национальной безопасности РФ до 2030 года выделяет информационную безопасность как стратегический национальный приоритет [6].

Положения статьи 16 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» также направлены на установление использования правовых, организационных и технических мер для обеспечения защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, соблюдения конфиденциальности информации ограниченного доступа, реализации права на доступ к информации [7]. Не менее актуальным для нашего исследования выступает Федеральный закон от 06 апреля 2011 № 63-ФЗ «Об электронной подписи» [8]. Электронная подпись, позволяя документам получать юридическую значимость, неразрывно связана с электронным документооборотом. Усиленная квалифицированная электронная подпись позволяет защитить документы от перехвата информации и от изменений после отправки, что является важным инструментом на пути к безопасному документообороту.

Исследование показало, что в рамках электронного документооборота механизмы защиты от основных угроз приобретают все большее значение. И в данном контексте опыт Федеральной налоговой службы Российской Федерации (далее – ФНС) имеет большое значение. В частности, в ФНС существует рабочая группа по разработке Концепции информационной безопасности при развитии электронного документооборота в хозяйственной деятельности, лидером которой является Фонд «Сколково» [9].

В Концепции определены меры и средства обеспечения защиты информации именно с привязкой к терминологии и к механизмам электронного документооборота. Анализ показал, что в проекте текста Концепции определяются основные рекомендации для операторов, разрабатывающих системы электронного документооборота. Например, на этапе проектирования таких систем необходимо учитывать требования, нормы и принципы защиты информации, причем на всех стадиях движения документа и его жизненного цикла. И хотя еще продолжается работа над разработкой данной концепции, факт того, что на федеральном уровне обсуждают вопросы защиты информации именно в контексте электронного документооборота, несомненно, радует. Данный факт только подтверждает актуальность нашего исследования.

Однако существующая нормативная база не позволяет гарантировать практическую безопасность важных данных. Коммерческие и некоммерческие организация постоянно сталкиваются с вызовами и угрозами от киберпреступников. Достаточно привести пример того, как 11 ноября 2021 года портал госуслуг подвергся одной из мощных кибератак. И хотя объектом атаки стал чат-бот, разработанный для консультирования пользователей и не имеющий доступа к персональным данным, как подчеркивали в Министерстве цифрового развития, связи и массовых коммуникаций РФ, страх утечки информации так или иначе присутствует, и этот случай лишь подтверждает наличие уязвимых мест системы. Не стоит забывать, что системы управления документооборотом тесно взаимодействуют с порталом госуслуг и с системой межведомственного электронного взаимодействия. При этом следует учитывать факт возможности заключения договоров дистанционно через портал госуслуг с использованием усиленной электронной подписи. А это является неотъемлемой частью электронного документооборота.

Из проведенного в процессе исследования анализа актуальных уязвимостей стоит отметить несколько тенденций современного 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 наиболее популярной точкой проникновения в системы при помощи социальной инженерии, которая, в свою очередь, всегда была и остаётся популярным инструментом киберпреступников.

Рассматривая данные тенденции, можно сделать вывод: действительно, сейчас веб-приложения являются наиболее уязвимыми системами, так как в секторе электронного документооборота они стали активно развиваться совсем недавно. Более того, уязвимы не только системы электронного документооборота – недостаток опыта работы с веб-приложениями сказывается и на ПО из других сфер. Одной из наиболее острых проблем веб-приложений является тот факт, что в 81% веб-приложений встречается некорректная настройка прав доступа, а также отсутствует защита от атак подбора учетных данных. Брутфорс – всё ещё актуальный инструмент, и отсутствие во многих сервисах защиты от такой популярной процедуры взлома упрощает работу злоумышленникам. Если обратить внимание на все исполнения систем электронного документооборота, то стоит отметить, что слабая парольная политика – всё ещё актуальная проблема и является одним из самых опасных недостатков. Несмотря на массовое информирование и консультации по укреплению парольной политики, это всё ещё глобальная угроза информационной безопасности практически всех средних и некоторых крупных компаний. 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.

В процессе исследования были проанализированы самые распространенные уязвимости внешнего и внутреннего периметра на основе данных, представленных JSOC CERT (рис. 2).

Самая распространенная уязвимость внешнего периметра (38%) – это CVE-2015-0204 (она же FREAK). Данная уязвимость была обнаружена в марте 2015 года в известном пакете свободно распространяемого ПО с открытыми исходными текстами под названием OpenSSL. Она позволяет злоумышленникам скомпрометировать используемое браузером защищенное подключение HTTPS. Уязвимости подвержены как клиентское, так и серверное ПО. В особенности это актуально для веб-версий систем электронного документооборота. Хотя стоит отметить, что не все системы снабжены SSL/TLS-сертификатами и всё ещё работают по протоколу HTTP, что является ещё большей угрозой.

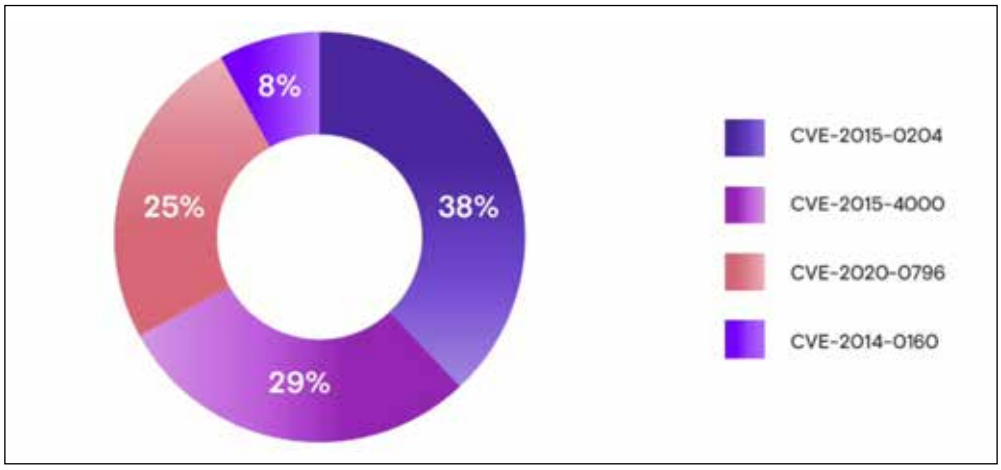

Рис. 2. Статистика уязвимостей внешнего периметра [10]

Далее идёт CVE-2015-4000 (она же Logjam, 29%) – компрометирующая TSL-соединения, по своей природе схожа с FREAK – то есть нацелена на веб-соединение. Несмотря на распространенность данных уязвимостей, их нельзя назвать критическими, так как их эксплуатация является достаточно сложной и специфической, для успешной атаки понадобится целый ряд сопутствующих факторов. Зато стоит отметить уязвимость CVE-2020-0796 (она же SMBGhost, 25%), которая затрагивает протокол Microsoft Server Message Block 3.1.1 (SMBv3). Данная уязвимость была обнаружена в марте 2020 года и является критической (позволяет повторить сценарий атак наподобие WannaCry или Petya) и актуальной, даже несмотря на патч от Microsoft.

Следующее направление, которое стоит обозначить – важность обновлений. По нашему мнению, это самая важная и глобальная проблема информационной безопасности, масштабнее, чем слабая парольная политика, фишинг или неправильно настроенное веб-приложение. А именно – время внедрения обновлений безопасности. В 92% организаций отсутствует ручной или полуручной процесс обновления ПО. Это катастрофически большой показатель, который сигнализирует о том, что большинство организаций всецело зависят от автоматических систем обновления ПО и, в случае обнаружения уязвимости, не смогут моментально внедрить патч. Учитывая, что электронный документооборот является достаточно чувствительной сферой и должен быть обеспечен максимальной информационной безопасностью, предположим, что всё же ПО систем электронного документооборота входят в оставшиеся 8%. Тем не менее мы всё равно сталкиваемся с другой большой проблемой: 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. Тем не менее в организациях всё ещё распространена так называемая культура стикеров. Некоторые сотрудники записывают важную информацию на бумаге и оставляют записки прямо на рабочем месте, зачастую на самом видном месте – приклеенными к монитору или на другие устройства периферии. Это означает, что советы по повышению информационной безопасности не работают должным образом, так как фундаментальные угрозы до сих пор допускаются, притом не только рядовыми пользователями, но и сотрудниками информационной безопасности. Хотя для данных отделов свойственна не столько «культура стикеров», сколько персональная некомпетенция сотрудников, выраженная ленью. Самый наглядный пример – среднее время установки обновлений – 45 дней.

Возвращаясь к безопасности внешнего периметра, стоит отметить следующие распространённые уязвимости.

– Некорректная настройка прав доступа. Является глобальной веб-проблемой. Нарушение структуры доступа пользователей открывает возможность для злоумышленников получить больше контроля над системой из-под не самых защищенных учетных записей.

– Раскрытие списка пользователей. Некоторым специалистам это не кажется критической угрозой, однако стоит помнить, что некоторые системы используют ID пользователя для распределения прав доступа, и, таким образом, злоумышленник может получить критическую информацию, эксплуатируя данный метод сортировки прав доступа.

– Внедрение SQL-кода. Такая атака позволяет получить информацию из базы данных веб-приложений и даже выполнять произвольные команды. В зависимости от других факторов данная атака может привести к проникновению во внутреннюю сеть или к компрометации клиентских данных.

– Использование учетных данных по умолчанию. Является глобальной проблемой в распространенных парольных политиках. Даже применяя требования на наличие символов верхнего, нижнего регистра, цифр и специальных символов, многие всё ещё подбирают пароли через брутфорс по словарям популярных комбинаций, что ещё раз доказывает наличие фактора лени среди пользователей.

Стоит отметить некоторые особенности обеспечения безопасности на внутреннем периметре. В нём также актуально использование паролей по умолчанию и некорректное управление паролями. Стоит отметить некорректно сконфигурированные средства защиты как одну из важных уязвимостей. Множество систем, в которых работает электронный документооборот, уже снабжены средствами защиты, однако их наличие не означает полную безопасность – необходима корректная настройка.

В процессе исследования обратимся к социотехническим исследованиям Solar JSOC, чтобы выяснить, насколько успешно применяется социальная инженерия (рис. 3).

Данные показывают, что среди злоумышленников самыми популярными «крючками» являются письма со ссылкой на веб-форму ввода данных, письма со ссылкой на веб-страницу и письма с вложенным docx-документом. 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. Безусловно, оставшиеся 65% пользователей не совершили потенциально опасных действий, тем не менее этот показатель всё ещё мал.

Очень важно отметить не только угрозы информационной безопасности как причины негативного влияния на функционирование организации, но и следствия. Например, утечки: компрометация конфиденциальных данных организации, которая покидает внутренний сектор и становится либо достоянием общественности, либо продается заинтересованным во вреде организации лицам, в том числе конкурентам. Особенно ощутимы потери, когда происходят утечки в сфере документооборота, ведь злоумышленники получают доступ к самой чувствительной информации: внутренним документам, инструкциям, особенностям работы организации, коммерческой тайне и т.п.

Опираясь на исследование, проведенное специалистами экспертно-аналитического центра InfoWatch, можно сделать вывод, что в 2020 году зафиксировано 2395 утечек данных из коммерческих, некоммерческих (государственных, муниципальных) организаций в различных странах мира. Это на 4,5% меньше, чем в 2019 году (2509 утечек), но на 5,8% превышает показатели 2018 года (2263). Причем 55,9% утечек были спровоцированы внешними нарушителями, 44,1% – внутренними (рис. 4). 35,4% утечек стали результатом действий и бездействия непривилегированных сотрудников [11].

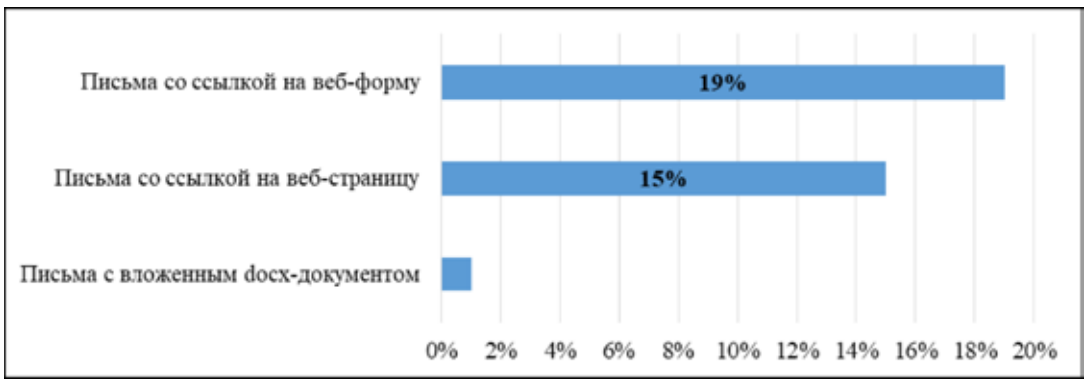

Рис. 3. Сотрудники, совершившие потенциально опасные действия (в %). Результаты социотехнического исследования [10]

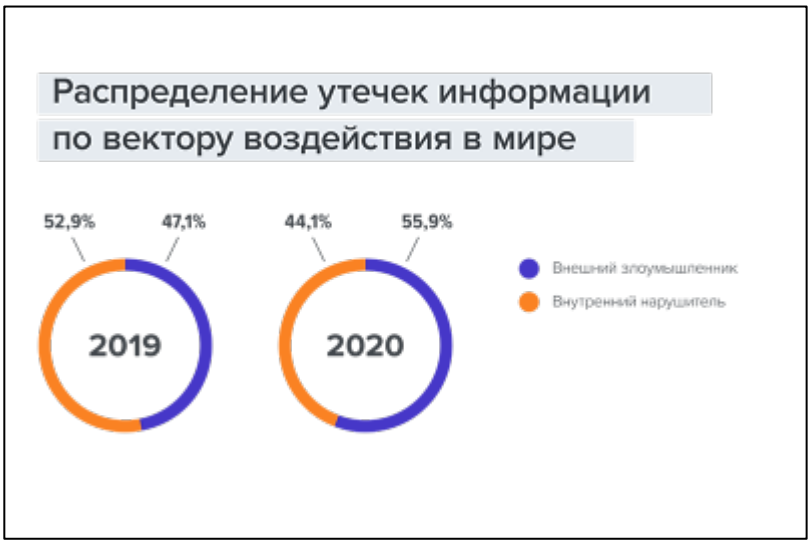

Рис. 4. Сравнительная статистика утечек в мире [11]

Также из данного отчета можно выделить тенденции роста внешних утечек и все большее приобретение умышленного характера. Анализируя данную статистику, следует изучить увеличение внешних утечек. Некоторые специалисты утверждают, что это означает рост квалификации киберпреступников, которым легче дается эксплуатация уязвимостей внешнего периметра. Однако данные показатели можно проанализировать и с другой точки зрения.

Можно предположить обратную ситуацию: квалификация киберпреступников с годами падает, и найти профессионала в данной сфере так же трудно, как найти высококвалифицированного специалиста информационной безопасности. Но инструментарий киберпреступников становится всё доступнее и проще в использовании – термин user-friendly стал актуален и для деятельности киберпреступников. Поэтому обострение успешных внешних атак вполне может быть обосновано не качеством, а количеством атакующих.

Почти все вышеописанные угрозы опираются на уязвимости software-сектора (ПО) или на человеческий фактор. Однако существуют уязвимости hardware-сектора – угрозы на уровне комплектующих компьютерных систем. И тут мы сталкиваемся с большой проблемой: весь потребительский сектор компьютерных комплектующих является импортным – на данном сегменте рынка почти нет российских представителей. Это влечёт за собой угрозу намеренно оставленных уязвимостей, которые могут быть использованы иностранными службами для получения низкоуровневого доступа к цифровым системам госструктур РФ. Поэтому, начиная с 2014 года, идет подготовка и реализация плана по импортозамещению вычислительной техники и микроэлектроники. Лидерами российского рынка являются компании АО «МЦСТ» (процессоры «Эльбрус») и АО «Байкал Электроникс» (процессоры «Байкал»). Обе компании производят микроэлектронику, однако позиционирование у них разное. Процессоры «Эльбрус» ориентированы на госсектор, так как предлагают работу в защищённом режиме – аппаратный контроль целостности структуры памяти, обеспечивающий информационную безопасность. Процессоры «Байкал» сильнее ориентированы на промышленные модули, различные сетевые устройства, например беспроводные маршрутизаторы, домашние маршрутизаторы, а также устройства автоматизации. К сожалению, в синтетических тестах российское оборудование проигрывает импортному, что не позволяет провести эффективное внедрение продукции на рынок домашних ПК, однако данная продукция позволяет повысить информационную безопасность госсектора на аппаратном уровне.

Но импортозамещение не ограничивается микроэлектроникой. Данный процесс призван установить новую фазу в информационном поле государственной сферы деятельности – цифровой суверенитет. Данный термин означает полную независимость от импортных цифровых решений и наличие собственных продуктов – как аппаратных, так и программных. Поэтому параллельно с планом по импортозамещению микроэлектроники идет планирование

и развитие стратегии импортозамещения программного обеспечения в госсекторе. Так, среди важного российского ПО стоит выделить СУБД Postgres. Данным ПО оснащены: Федеральная налоговая служба, Министерство финансов Российской Федерации, Сбербанк, Газпром и другие крупные компании и ведомства.

Но в политике импортозамещения также можно отметить и неэффективные задачи. Например, 10 марта 2021 года стало известно об инициативе Минцифры запретить иностранный софт в школах РФ. Подобные задачи контрпродуктивны, и радикальные протекционистские меры не способны изменить ситуацию. Более того, существует техническое противоречие – все отечественные операционные системы основаны на Linux, что значительно сужает круг офисных решений и иного ПО, необходимого для современного образовательного процесса. Также учителям приходится работать с несколькими платформами, и половина из них – от иностранных разработчиков. Всё это приводит к снижению эффективности и не является грамотным ведением политики импортозамещения.

Заключение

Обобщая результаты проведенного анализа, можно сделать вывод, что проблемы обеспечения информационной безопасности при реализации электронного документооборота переходят в новую плоскость. На основе проведенного исследования были выделены актуальные уязвимости, которые можно классифицировать по следующим основным признакам:

- реализация дистанционного формата работы характеризуется переходом большинства компаний с толстых клиентов на соответствующие web-приложения;

- применение мобильных приложений для реализации функций электронного документооборота не обеспечивается соответствующим уровнем безопасности;

- слабая парольная политика компаний и организаций остается одной из самых актуальных глобальных угроз, несмотря на массовое информирование и консультации специалистов;

- уязвимости внешнего периметра: использование свободно распространяемого ПО с открытыми исходными текстами, и сейчас это особенно актуально для вебверсий систем электронного документооборота; некорректная настройка прав доступа; использование учетных данных по умолчанию; раскрытие списка пользователей;

- уязвимости внутреннего периметра: некорректное управление паролями, некорректно сконфигурированные средства защиты;

- среднее время автоматической установки обновлений систем безопасности.

Таким образом, мы убеждаемся в необходимости новых подходов к защите систем электронного документооборота. Важно понимать, что полностью исключить киберпреступления невозможно, но вполне реально принять все необходимые меры для минимизации рисков при реализации деятельности в цифровом пространстве. Предлагаем рассмотреть следующие задачи:

- усилить меры по разработке средств и методов обеспечения информационной безопасности именно с привязкой к терминологии и механизмам электронного документооборота;

- определить единый механизм требовании для вендоров и интеграторов, разрабатывающих и внедряющих системы электронного документооборота в области ИБ;

- усилить парольную политику на уровне управления и реализовывать на постоянной основе мероприятия по обучению персонала в рамках проектов «Киберучения».

В процессе проведенного исследования можно также сделать вывод, что все вышеописанные меры являются в большей степени административными аспектами повышения уровня информационной безопасности во всём госсекторе, включая и системы электронного документооборота. Вкупе с технической частью исследования можно ещё раз убедиться в том, насколько обеспечение информационной безопасности является комплексным процессом, требующим высокой квалификации сотрудников: как рядовых, так и специалистов по безопасности, а отсутствие информационной безопасности способно привести к утечкам чувствительных данных, которые могут повлечь за собой катастрофические потери.

Список литературы

1. Мирошниченко М.А., Бондаренко А.А. Пиналова Е.В. Актуальные проблемы обеспечения информационной безопасности систем электронного документооборота в рамках цифровой трансформации // Вестник академии знаний. 2020. № 1(36). С. 137-142.

2. Евдокимова Л.М., Корябкин В.В., Пылькин А.Н., Швечкова О.Г. Электронный документооборот и обеспечение безопасности стандартными средствами windows: учебное пособие. М.: КУРС, 2019. 296 с.

3. Актуальные киберугрозы: III квартал 2021 года // Исследование компании Positive Technologies. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/ (дата обращения: 12.12.2021).

4. Распоряжение Правительства Российской Федерации от 28.07.2017 №1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 08.12.2021).

5. Информационная безопасность // Официальный сайт Министерства цифрового развития, связи и массовых коммуникация Российской Федерации. [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/874/ (дата обращения: 08.12.2021).

6. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 08.12.2021).

7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 08.12.2021).

8. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (последняя редакция). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 08.12.2021).

9. Распоряжение ФНС России от 13.11.2020 n 322 (ред. От 11.04.2021) «О подгруппах по направлениям развития электронного документооборота с представителями бизнес-сообщества». [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/el_bus_entities/10927823/ (дата обращения: 08.12.2021).

10. Отчет об атаках и инструментарии профессиональных кибергруппировок в 2021 году // Исследование экспертов Solar JSOC. [Электронный ресурс]. URL: https://rt-solar.ru/analytics/reports/2501/ (дата обращения: 10.12.2021).

11. Исследование утечек информации ограниченного доступа в 2020 году // Компания InfoWatch. [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu/ (дата обращения: 12.12.2021).