УДК 346.7

Николаев Эрик Викторович

студент магистратуры
Российский государственный
гуманитарный университет
Москва, Россия
eraikeking1@yandex.ru

Erik V. Nikolaev

Post-graduate student
Russian State University for the Humanities
Moscow, Russia

НЕКОТОРЫЕ ВОПРОСЫ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

SOME QUESTIONS ABOUT INFORMATION SECURITY IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Аннотация

В статье рассматриваются вопросы информационной безопасности и защиты информации. Даётся характеристика организации защиты информации в системах электронного документооборота. Определяются угрозы безопасности информации. Даётся оценка возможности получения несанкционированного доступа к информации. Приводится характеристика комплекса мероприятий по обеспечению защиты информации. Рассматривается использование облачных технологий для повышения степени защиты информации. Определяются дальнейшие пути развития информационной безопасности. Оценивается возможность применение искусственного интеллекта для обеспечения защиты информации.

Ключевые слова:

информационное право, информационная безопасность, системы электронного документооборота, защита информации

Abstract

The article discusses the issues of information security and data protection. The characteristic of the organization of information protection in electronic document management systems is given. Information security threats are identified. The assessment of the possibility of obtaining unauthorized access to information is given. The description of the complex of measures to ensure the protection of information is given. The use of cloud technologies to increase the degree of information security is being considered. Further ways of developing information security are being determined. The possibility of using artificial intelligence to ensure information security is being evaluated.

Keywords:

information law, information security, electronic document management systems, data protection

Системы электронного документооборота (СЭД) – это уже довольно давно неотъемлемая часть управленческой структуры любого предприятия или даже государственного органа. СЭД позволяет в первую очередь уменьшить то количество времени, которое требуется для обработки документов, будь то кадровая документация, связанная с «передвижением» внутри организации сотрудников или управленческие документы, которые несут в себе различного рода поручения и задачи для выполнения. Также всё это уменьшает экономические издержки на данные операции.

С самого первого упоминания об электронных документах звучит вопрос, который имеет актуальность и по сегодняшний день: «может ли СЭД обеспечить

безопасность информации, которая содержится в электронном виде?». Потому что нередко в СМИ можно видеть заголовки о хакерских атаках на сервера крупных компаний. Правда в том, что 100% гарантию от взлома не может обеспечить ни один системный протокол, так как здесь всё закономерно: чем лучше способы защиты информации, тем совершеннее способы обхода защитных протоколов.

Но несанкционированный доступ к информации может быть получен не только в ходе взлома серверов. Банальная халатность сотрудников может стать проблемой для крупной организации или ведомства. Многие слышали про такой инструмент цифровизации как «электронная подпись (ЭП)». В целях расширения представления у граждан об этом стоит отметить, что электронная подпись бывает простой, то есть нет необходимости её получения через специальные центры. Простой ЭП называется «логин» и «пароль» от аккаунта, например, электронной почты или в любом Интернет-ресурсе. Так и в организациях и ведомствах для входа в свой личный кабинет на рабочем месте сотрудники используют простую электронную подпись. Именно это может стать тем каналом утечки данных через сотрудников, о котором написано выше. Отсюда может начаться целая цепочка вредоносных действий.

Главным вредоносным действием является получение доступа к серверам информации. Злоумышленник, получивший данные для входа на сервер, получает возможность завладеть документальной информацией организации, которые представляют особую ценность. Это информация от уставных документов до личных данных всех сотрудников организации или граждан, которые в данной организации обслуживаются, например, если речь идёт о многофункциональных центрах или порталах предоставления государственных и муниципальных услуг. В информационной среде принято считать, что информация, к которой удалось получить несанкционированный доступ, перестаёт представлять те ценность и качество, которые были изначально в неё заложены [1, с. 50-51].

Однако, эксперты считают, что самый простой способ получения доступа к информации не является самым распространённым. Чаще всего атаки осуществляются на транспортные информационные каналы, по которым осуществляется взаимодействие как внутри организации, так и между организацией и её пользователями. Но ещё чаще подвергаются взлому мессенджеры и электронная почта. Эти способы передачи информации не относятся к СЭД, а значит те протоколы защиты, которые используются там, здесь не применяются. По сути, ответственность

возлагается на организацию и является отдельной мерой обеспечения защиты информации. Далее рассмотрим некоторые из этих мер.

Комплекс мероприятий по обеспечению защиты, как и любой другой организационный элемент предприятия, начинается с разработки соответствующий нормативных актов, в которых указаны этапы и процедуры обеспечения защиты информации, а также инструкции для сотрудников. Если речь идёт о СЭД, то здесь на себя ответственность берут сами разработчики. Согласно заключённым договорам, именно в их обязанности входит не только обучение персонала работе с системой, но и инструктаж по обеспечению безопасности в процессе выполнения должностных обязанностей в системах [2, с. 137-142; 3, с. 77].

Следующий этап защиты носит физический характер, т.е. охрана самого рабочего помещения. Это системы видеонаблюдения, пункты охраны в организации, установка дверей с использованием пропускной системы и т.д. Однако, данные меры уже являются устаревшими, так как в последние годы в большинстве организаций офисная работа является основным видом осуществления деятельности. Всё больше преобладает возможность организации удалённой работы. А данный комплекс мероприятий не распространяется на рабочие места сотрудников, оборудованные у них дома.

Этот момент стоит выделить как основной недостаток удалённой работы, так как организация не предусматривает обеспечение защиты места проживания сотрудника откуда он осуществляет свою деятельность. Это означает, что информационная безопасность в этом случае является личной ответственностью самого сотрудника организации или ведомства. В конечном счёте это выражается в так называемой «бреши» в системе защиты информации.

Теперь перейдём к основному комплексу мероприятий – технических мер. Это такие средства защиты информации, как фаерволы, антивирусы, системы обнаружения вторжений, которые и позволяют быстро среагировать на возможные попытки взлома, и многие другие. К техническим мерам также относятся и средства защиты при работе с самой документированной информацией. Например, это аутентификация и использование шифровальных кодов. В последние годы во всём мире активно развиваются облачные технологии. Говоря простыми словами – это виртуальный сервер для хранения информации. Но его можно использовать и как инструмент защиты информации, позволяя создавать резервные копии данных, что

является возможностью быстрого восстановления всей необходимой информации при утрате основных баз данных. Но даже «облако» не способно гарантировать полную безопасность [4, с. 42; 5, с. 49; 6, с. 576-579].

Как уже было отмечено раньше, чем надёжнее защита информации, тем совершеннее попытки получения доступа к ней. Это означает, что даже современные облачные технологии не могут дать 100% гарантии обеспечения защиты информации. Здесь может прийти на помощь внедрение систем искусственного интеллекта. Многими специалистами отмечается, что внедрение ИИ позволит автоматизировать большинство процессов в организации, в том числе и процедуры защиты информации. Если сейчас за всеми программами и протоколами защиты данных следит специалист, то ИИ позволит это будет делать автоматически. И в качестве основного преимущества здесь выступит сокращение времени на определения проникновения в системы организации, что позволит быстрее принять решение по предотвращению такой попытки. Но, опять же, «чем надёжнее защита…», есть вероятность, что и это не будет давать гарантии полностью обеспечить защиту данных.

Подведём итоги вышесказанного. Политика безопасности должна являться первостепенной функцией любой организации и ведомства. Чем выше значимость хранимой на сервере информации, тем современнее и надёжнее должны быть протоколы её защиты. Исследование позволило выявить, что полностью предотвратить попытки взлома невозможно. Но проведение постоянного мониторинга кибербезопасности позволяет сократить риски взлома и минимизировать последствия кибератак.

Системы электронного документооборота не только повышают качество работы организации в целом, но и способствуют повышению надёжности защиты информации. Как показывает практика, передача данным посредством информационных каналов намного надёжнее традиционных способов посредством курьеров и почтой. Как минимум, значимые документы передаются с одного сервера на другой, что уменьшает то количество лиц, которые имеют к ним доступ.

Современные протоколы шифрования данных позволяют обеспечить хранение наиболее значимой информации и предотвратить практически любые попытки получения доступа к ней. Развитие информационных технологий в будущем позволит создавать наиболее передовые системы обнаружения угроз, которые будут устранять

эти самые угрозы до того момента, как злоумышленники получать доступ к ценной для организаций, общества и государства в целом информации.

Список использованных источников

1. Гордиенко, Е. П. Проблема защиты информации и информационной безопасности в системах электронного документооборота / Е.П. Гордиенко // Транспорт: наука, образование, производство ("Транспорт-2024"): Воронеж: Ростовский государственный университет путей сообщения, 2024. С. 48-54.

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

3. Морозова М. Ю. Обеспечение информационной безопасности в системах электронного документооборота / М.Ю. Морозова, П.С. Фомина // Международный студенческий научный вестник. 2023. № 6. С. 77.

4. Назиев М. И. Сущность и проблемы обеспечения информационной безопасности системы электронного документооборота в современной организации / М И. Назиев, Л.Р. Магомаева // Махачкала: ФОРМАТ, 2023. С. 40-44.

5. Перова М. В. Обеспечение информационной безопасности в системах электронного документооборота / М.В. Перова, Д.А. Пономарев // Фундаментальные исследования. 2022. № 2. С. 46-54.

6. Филяк П. Ю. Обеспечение информационной безопасности при использовании систем электронного документооборота/ECM-систем / П.Ю. Филяк, М.О. Бартов, А.В. Красномовец // Информация и безопасность. 2015. № 4. С. 576-579.