www.volsu.ru

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.3.4

УДК 004.056.5:003.26
ББК 32.972.53

ОЦЕНКА ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ И ОРГАНИЗАЦИОННЫХ МЕР ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ АНАЛИЗА РЕАЛЬНЫХ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

Владислав Георгиевич Яриков

Кандидат педагогических наук,
доцент кафедры методики преподавания математики и физики, ИКТ,
Волгоградский государственный социально-педагогический университет
yarikov_vg@mail.ru
просп. им. Ленина, 27, 400005 г. Волгоград, Российская Федерация

Вадим Сергеевич Кулезнев

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-241_673422@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье проведена оценка эффективности криптографических и организационных мер защиты систем электронного документооборота (ЭДО) на основе анализа реальных компьютерных инцидентов. Рассмотрены ключевые нормативные документы РФ, определены криптографические и организационные меры защиты, проведен их качественный анализ. Проанализированы реальные инциденты в сфере ЭДО, выявлены причины неэффективности отдельных мер и сформулированы рекомендации по совершенствованию комплексной защиты.

Ключевые слова: электронный документооборот, информационная безопасность, криптографическая защита, организационные меры, электронная подпись, шифрование, разграничение доступа, инциденты.

© Яриков В.Г., Кулезнев В.С., 2025

Введение

Активное внедрение электронного документооборота (далее – ЭДО) в государственном и корпоративном секторах сопровождается ростом числа киберинцидентов, направленных на несанкционированный доступ к конфиденциальной информации, подмену документов и компрометацию каналов связи. ЭДО представляет собой совокупность процессов и средств для создания, передачи, хранения и обработки документов в цифровой форме. Защита таких систем требует комплексного применения как криптографических, так и организационных мер [3; 8].

Криптографические меры обеспечивают математическую стойкость к несанкционированному доступу, включают использование электронной подписи (далее – ЭЦП) для подтверждения подлинности документов и шифрование для обеспечения конфиденциальности.

Организационные меры включают регламенты, разграничение доступа, политику информационной безопасности, обучение персонала и мониторинг событий. Они направлены на минимизацию человеческого фактора и обеспечение корректного использования технических средств защиты.

Российская нормативная база задает основы обеспечения безопасности ЭДО. Федеральный закон № 152-ФЗ «О персональных данных» регулирует обработку персональных данных и устанавливает требования к их защите. Федеральный закон № 63-ФЗ «Об электронной подписи» определяет виды ЭП и их юридическую значимость. ГОСТ Р 57580.1-2017 описывает базовый состав организационных и технических мер защиты для финансовых организаций [2; 7; 8].

Цель данной работы – провести качественную оценку эффективности криптографических и организационных мер защиты ЭДО на основе анализа реальных компьютерных инцидентов и выработать рекомендации по совершенствованию практик защиты.

Криптографические меры защиты в системах ЭДО

Криптографическая защита является ключевым элементом обеспечения безопасности ЭДО. Она направлена на защиту конфиденциальности, целостности и подлинности электронных документов. К основным криптографическим средствам относятся электронная подпись (ЭЦП) и шифрование данных [6].

ЭЦП подтверждает авторство и неизменность электронного документа. Квалифицированная электронная подпись, выданная аккредитованным удостоверяющим центром, приравнивается к собственноручной подписи на бумажных носителях и имеет юридическую силу в соответствии с Федеральным законом № 63-ФЗ [7]. Эффективность ЭЦП зависит от надежного хранения закрытых ключей и корректной организации процедур их выдачи и отзыва. Нарушение этих процессов может привести к компрометации подписи и совершению юридически значимых действий третьими лицами.

Шифрование применяется для защиты документов как при передаче, так и при хранении. Используются протоколы защищенной передачи данных (например, HTTPS/TLS) и механизмы сквозного шифрования, когда документы шифруются на стороне отправителя и расшифровываются только получателем.

Российское законодательство обязывает использовать сертифицированные средства криптографической защиты информации (СКЗИ) для обработки персональных данных и другой конфиденциальной информации [9]. Однако шифрование не предотвращает утечки, если злоумышленник получает доступ к системе с легальными правами пользователя. В таких случаях защита должна опираться также на организационные меры: разграничение доступа, мониторинг и аудит действий пользователей.

Организационные меры защиты в системах ЭДО

Организационные меры дополняют криптографические, обеспечивая контроль над использованием технологий и минимизацию человеческого фактора. Их применение позволяет снизить риск инцидентов, связанных с ошибками персонала, нарушением регламентов или внутренними злоупотреблениями [5].

Принцип минимальных привилегий требует предоставления каждому пользователю только необходимых прав. Реализация этого принципа включает назначение ролей, настройку доступа к документам и регулярный аудит прав.

Четко сформулированные правила обращения с информацией повышают защищенность систем. Политика информационной безопасности определяет категории документов, способы их защиты, порядок предоставления доступа, требования к паролям и действия при инцидентах. Разработка и доведение таких регламентов до сотрудников обеспечивает предсказуемое и контролируемое поведение

пользователей, снижая риск случайных или умышленных нарушений.

Журналирование действий пользователей и системных событий позволяет выявлять аномалии, расследовать инциденты и сдерживать потенциальных нарушителей. Регулярный анализ логов помогает своевременно обнаруживать несанкционированные действия, утечки или попытки взлома. Механизмы мониторинга особенно важны для раннего выявления сложных атак. Без надлежащего мониторинга организация может узнать об инциденте только после нанесения ущерба.

По статистике, большинство инцидентов связано с человеческим фактором [4; 5]. Обучение сотрудников правилам безопасной работы с ЭДО, проведение инструктажей, проверок и тестов повышает уровень «кибергигиены».

Например, атаки с использованием вредоносных вложений в электронных документах часто успешны именно из-за отсутствия у сотрудников навыков распознавания опасных файлов. Регулярное обучение снижает риск таких инцидентов.

Анализ реальных компьютерных инцидентов в сфере ЭДО

В аналитических обзорах ИБ-компаний 2023–2025 гг. можно выделить устойчивую тенденцию: большинство инцидентов, связанных с системами электронного документооборота (ЭДО), обусловлены организационными уязвимостями – ошибками в разграничении доступа, неправильным управлением жизненным циклом ЭЦП и низким уровнем кибергигиены – а не взломом криптографических алгоритмов.

Так, в отчете Positive Technologies «Утечки конфиденциальных данных из организаций: актуальные угрозы второго полугодия 2024 года» проанализированы десятки публично раскрытых утечек и объявления с теневых форумов. В этом отчете отмечается, что значительная доля утечек документов и баз данных происходит через компрометацию учетных записей, подрядчиков и каналов взаимодействия ЭДО, а не через взлом криптосистем [5].

В исследовании Positive Technologies за первое полугодие 2024 г. («Утечки данных в первой половине 2024 года») выделяется тенденция к распространению атак с помощью внутренних аккаунтов: злоумышленники используют легитимные человеческие учетные записи, чтобы маскировать свои действия, экспортировать документы и скрываться среди обычной активности. В некоторых случаях использовались стандартные мессенджеры как управляющие каналы, что позволяло обходить сетевые фильтры и сливаться с фоновым трафиком [4].

В отчете Group-IB Trends Report 2025 указывается, что в 2024 г. было зафиксировано 828 атак APT, что на 58 % больше, чем в предыдущем году, и что такие атаки все чаще нацеливаются не на инфраструктуру, а на внутренние системы, включая документооборот и передачи данных между узлами [10]. Хотя прямых публичных кейсов взломов ЭДО в отчете нет, рост активности APT подчеркивает необходимость усиления защиты даже в «тихих» сервисах обмена документами.

Конкретные российские кейсы в открытом доступе из сферы ЭДО встречаются реже, но в материалах СМИ и профессиональных блогах зафиксированы следующие типичные сценарии:

– утечки через сотрудников технической поддержки, когда им выдавались избыточные права доступа к документам клиентов;

– рассылка через ЭДО документов с вредоносными макросами или скриптами, мимикрирующими под служебные сообщения;

– подмены или выдачи ЭЦП на основе поддельных документов, что позволяло выполнять юридически значимые операции от имени жертвы (в некоторых случаях эти схемы обнаруживались и документировались в СМИ) [1].

Из этих кейсов вытекают важные уроки: криптографические средства (ЭЦП, шифрование) остаются фундаментом защиты, однако утечки документированных потоков и подмены ЭЦП чаще всего происходят на уровнях, где технологии взаимодействуют с людьми и процессами. Если организация не контролирует выдачу подписей, не ведет аудит действий, не ограничивает привилегии и не обеспечивает обучение

персонала – то криптооснова может быть обойдена.

Поэтому анализ инцидентов 2023–2025 гг. подтверждает: для надежной защиты ЭДО необходим комплексный подход, при котором криптографические средства реализованы корректно, а организационная часть – выстроена строго и динамично совершенствуется. Это включает:

– надежную процедуру верификации при выдаче ЭЦП, обязательное уведомление владельцев подписи;

– принцип минимальных привилегий, регулярный аудит и ревизию прав доступа;

– мониторинг и корреляцию журналов событий с целью выявления подозрительной активности;

– обучение сотрудников методам распознавания фишинга и вредоносных документов;

– фильтрацию вложений в ЭДО и проверку макросов/скриптов перед открытием.

Заключение

Эффективная защита электронного документооборота требует комплексного применения криптографических и организационных мер.

Криптографические механизмы, такие как ЭЦП и шифрование, обеспечивают высокий уровень математической защиты данных. Однако их эффективность снижается при отсутствии надежных организационных процедур – разграничения доступа, мониторинга, политики безопасности и обучения персонала.

Реальные инциденты показывают, что компрометация ключей ЭЦП, ошибки доступа и человеческий фактор являются основными причинами нарушений безопасности. Для повышения устойчивости систем ЭДО необходимо:

– поддерживать актуальность нормативной базы и средств криптографической защиты;

– реализовывать принцип минимальных привилегий и контроль доступа;

– вести журналирование и мониторинг событий безопасности;

– регулярно обучать сотрудников и проверять соблюдение правил.

Только комплексное сочетание технических и организационных мер позволяет обеспечить надежную защиту электронного документооборота.

СПИСОК ЛИТЕРАТУРЫ

1. В Татарстане фиксируется рост преступлений с использованием поддельных ЭЦП // Реальное время. – 05.08.2023. – Электрон. текстовые дан. – Режим доступа: https://realnoevremya.ru/articles/361399

2. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – М. : Стандартинформ, 2017. – 66 с.

3. Как Documentolog обеспечивает информационную безопасность в облаке. – 2019. – Электрон. текстовые дан. – Режим доступа: https://documentolog.com/blog/kak-documentolog-obespechivaet-informatsionnuyu-bezopasnost-v-oblake

4. Утечки данных в первой половине 2024 года // Positive Technologies. – 2024. – Электрон. текстовые дан. – Режим доступа: https://ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-v-pervoj-polovine-2024-goda/

5. Утечки конфиденциальных данных из организаций: актуальные угрозы второго полугодия 2024 года // Positive Technologies. 2024. – Электрон. текстовые дан. – Режим доступа: https://ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-aktualnye-ugrozy-vtorogo-polugodiya-2024-dlya-organizacij/

6. Файзулаев, Д. Ф. Методы и средства анализа рисков информационной безопасности предприятия / Д. Ф. Файзулаев, Б. Б. Морозов // Безопасность информационных технологий. – 2017. – Т. 24, № 3. – С. 69–74.

7. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». Доступ из справ.-правовой системы «КонсультантПлюс».

8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Доступ из справ.-правовой системы «КонсультантПлюс».

9. Черняев, М. Д. Методика оценки риска EBIOS / М. Д. Черняев // Управление развитием крупномасштабных систем (MLSD'2023). – М. : ИПУ РАН, 2023. – С. 1240–1243.

10. Threat Intelligence Report 2025 // Group-IB. – 2025. – Электрон. текстовые дан. – Режим доступа: https://www.group-ib.com/resources/threat-intelligence-report-2025/

REFERENCES

1. V Tatarstane fiksiruetsya rost prestupleniy s ispolzovaniem poddelnykh ETsP [Tatarstan Sees an

Increase in Crimes Using Fake Electronic Signatures]. *Realnoe vremya*, 2023, Aug. 5. URL: https://realnoevremya.ru/articles/361399

2. *GOST R 57580.1–2017. Bezopasnost finansovyh (bankovskih) operatsiy. Zashchita informatsii finansovyh organizatsiy. Bazovy sostav organizatsionnyh i tekhnicheskih mer* [Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Basic Set of Organizational and Technical Measures]. Moscow, Standartinform Publ., 2017. 66 p.

3. *Kak Documentolog obespechivaet informatsionnuyu bezopasnost v oblake* [How Documentologist Ensures Information Security in the Cloud], 2019. URL: https://documentolog.com/blog/kak-documentolog-obespechivaet-informatsionnuyu-bezopasnost-v-oblake

4. Utechki dannykh v pervoy polovine 2024 goda [Data Leaks in the First Half of 2024]. *Positive Technologies*, 2024. URL: https://ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-v-pervoj-polovine-2024-goda/

5. Utechki konfidentsialnykh dannykh iz organizatsiy: aktualnye ugrozy vtorogo polugodiya 2024 goda [Confidential Data Leaks from Organizations: Current Threats of the Second Half of 2024]. *Positive Technologies*, 2024. URL: https://ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-aktualnye-ugrozy-vtorogo-polugodiya-2024-dlya-organizacij/

6. Faizulayev D.F., Morozov B.B. Metody i sredstva analiza riskov informatsionnoy bezopasnosti predpriyatiya [Methods and Means of Information Security Risk Analysis for an Enterprise]. *Bezopasnost informatsionnyh tehnologiy*, 2017, vol. 24, no. 3, pp. 69-74.

7. Federalnyy zakon ot 06.04.2011 № 63-FZ «Ob elektronnoy podpisi» [Federal Law No. 63-FZ of April 6, 2011 "On Electronic Signature"]. *Access from Reference Legal System "KonsultantPlyus"*.

8. Federalnyy zakon ot 27.07.2006 № 152-FZ «O personalnyh dannyh» [Federal Law No. 152-FZ of July 27, 2006 "On Personal Data"]. *Access from Reference Legal System "KonsultantPlyus"*.

9. Chernayev M.D. Metodika otsenki riska EBIOS [EBIOS Risk Assessment Methodology]. *Upravleniye razvitiyem krupnomasshtabnyh sistem (MLSD'2023)*. Moscow, IPU RAN, 2023, pp. 1240-1243.

10. Threat Intelligence Report 2025. *Group-IB*, 2025. URL https://www.group-ib.com/resources/threat-intelligence-report-2025/

EVALUATION OF THE EFFECTIVENESS OF CRYPTOGRAPHIC AND ORGANIZATIONAL MEASURES TO PROTECT ELECTRONIC DOCUMENT MANAGEMENT BASED ON THE ANALYSIS OF REAL COMPUTER INCIDENTS

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Methods of Teaching Mathematics and Physics, ICT,
Volgograd State Social and Pedagogical University
yarikov_vg@mail.ru
Prosp. Lenina, 27, 400005 Volgograd, Russian Federation

Vadim S. Kuleznev

Student, Department of Information Security,
Volgograd State University
IBm-241_673422@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article assesses the effectiveness of cryptographic and organizational measures to protect electronic document management (EDM) systems by analyzing real-world computer incidents. The authors review key Russian regulatory documents, define relevant cryptographic and organizational measures, and conduct their qualitative analysis.

The cryptographic framework includes the use of electronic digital signatures (EDS) and encryption, ensuring data confidentiality, integrity, and authenticity. Organizational measures encompass access control, security policies, user training, and activity monitoring, aimed at mitigating the human factor. The core of the study is an analysis of recent incidents (2023–2025) based on reports from leading cybersecurity companies. The analysis reveals a consistent trend: most EDM security breaches stem from organizational vulnerabilities – such as excessive privileges, poor EDS lifecycle management, and lack of user awareness – rather than from breaches of cryptographic algorithms themselves. Incidents often involve compromised accounts, insider threats, and social engineering. The conclusion emphasizes that while cryptographic tools provide an essential mathematical security foundation, their effectiveness is critically dependent on robust organizational practices. For reliable EDM protection, a holistic approach is necessary, integrating up-to-date cryptographic means with strict implementation of the principle of least privilege, comprehensive logging and monitoring, and regular employee training. Recommendations for improving the security posture of EDM systems are formulated based on the identified incident patterns.

Key words: electronic document management, information security, cryptographic protection, organizational measures, electronic signature, encryption, access control, incidents.