

*Ласковая В.С.,*

*студент,*

*4 курс, факультет «Правовое обеспечение*

*национальной безопасности»*

*Оренбургский институт (филиала)*

*Университета имени О. Е. Кутафина (МГЮА)*

*Россия, г. Оренбург*

*Научный руководитель: Кузьмина М.В.,*

*кандидат юридических наук,*

*доцент кафедры предпринимательского и трудового права*

*Оренбургский институт (филиала)*

*Университета имени О. Е. Кутафина (МГЮА)*

*Россия, г. Оренбург*

## **ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ**

*Аннотация:* В статье рассматриваются вопросы информационной безопасности российских организаций в условиях роста киберугроз. Акцент сделан на защите персональных данных. Анализируются угрозы для СЭД на этапах жизненного цикла документов и их источники. Представлен комплекс правовых, организационных мер защиты с учётом требований федеральных законов. Подчеркивается, что четкая система информационной безопасности снижает финансовые риски, и повышает конкурентоспособность организации.

*Ключевые слова:* электронная система делопроизводства, риски для информационной безопасности, сохранность данных, неизменность данных,

непрерывность доступа к данным, цифровая безопасность, проверка соответствия требованиям информационной безопасности, аутентификация из двух факторов, криптографическая защита информации.

**Annotation:** *The article addresses issues of information security for Russian organizations in the context of growing cyber threats. The focus is on the protection of personal data. Threats to electronic document management systems (EDMS) are analyzed at various stages of the document lifecycle and their sources are identified. A set of legal and organizational security measures is presented, taking into account the requirements of federal laws. It is emphasized that a robust information security system reduces financial risks and enhances the organization's competitiveness.*

**Key words:** *electronic document management system; information security risks; data integrity; data immutability; data availability; digital security; information security compliance audit; two factor authentication; cryptographic data protect.*

Огромную важность сегодня приобретают вопросы и проблемы информационной безопасности для российских организаций в условиях нестабильной политической обстановки, террористических актов и информационной пропаганды. В результате утечек информационных ресурсов при злонамеренных воздействиях компании страдают от незащищённости имеющейся информации.

Гафнер В. В. трактует информационную безопасность как защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или

искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.<sup>1</sup>

Для защиты коммерческой деятельности на уровне информационных систем и персональных данных ключевой задачей является снижение вероятности финансовых издержек, которые могут возникнуть из-за нарушений конфиденциальности, целостности или доступности обрабатываемой информации. Особое внимание уделяется охране личных сведений граждан, поскольку их несанкционированное раскрытие чревато юридическими проблемами и подрывом доверия со стороны клиентов.

Доступ к данным строго контролируется и предоставляется только соответствующим сотрудникам, чей уровень полномочий позволяет работать с ними. Информация поддерживается в неизменном виде на всех этапах её жизненного цикла (сбор, обработка, хранение, передача), предотвращая искажения и подтверждая её точность.<sup>2</sup>

Для компаний вопросы информационной безопасности неразрывно связаны с их системами электронного документооборота (СЭД). СЭД представляет собой организационно-технический комплекс, предназначенный для создания, управления доступом и распространения электронных документов в рамках компьютерных сетей. Она также осуществляет контроль за перемещением документов внутри организации.

Ключевая цель СЭД – повышение общей эффективности работы компании путем автоматизации документооборота и взаимодействия между сотрудниками. Кроме того, СЭД способствует интеграции работы различных отделов, тем самым ускоряя выполнение задач. Следовательно, система электронного документооборота должна играть центральную роль в аспектах информационной безопасности компании.

---

<sup>1</sup> Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов н/Д: Феникс, 2010. — 324 с.

<sup>2</sup> Международный научный журнал «ВЕСТНИК НАУКИ» № 11 (92) Том 3. 2025 г. 915 - 916 с.

Тем не менее, следует отметить, что ни одна модель СЭД не застрахована полностью от внешних и внутренних угроз. В связи с этим, далее будут рассмотрены угрозы информационной безопасности, способные нанести ущерб электронному документообороту.

По мнению исследователей Басырова Р. Р. и Прашина К. А., угрозы СЭД могут возникать на разных этапах жизненного цикла документов, включая их создание, получение, исполнение и отправку.<sup>3</sup>

Источниками угроз могут выступать различные субъекты, такие как конкуренты, преступники или коррумпированные лица, стремящиеся получить доступ к защищенной информации, изменить ее в корыстных целях или нанести материальный ущерб.

В результате проведенного исследования были разработаны меры по предотвращению угроз информационной безопасности в СЭД.

Помимо прочего, обеспечение защиты информационных ресурсов компании требует регулярного аудита информационной безопасности, который позволяет получить объективную оценку уровня защищенности от киберугроз.<sup>4</sup> Также критически важно установить требования к защите электронных данных, включая шифрование конфиденциальной информации. Идентификация личности сотрудников через персональные коды доступа также является важным элементом обеспечения безопасности СЭД.<sup>5</sup>

Комплекс мер защиты включает в себя: разработку внутренних политик и регламентов туда входят положения об обработке персональных данных, инструкции по доступу, должностные обязанности; проведение регулярных тренингов для персонала по основам кибербезопасности (методы фишинга, социальная инженерия); шифрование данных при хранении и передаче с

---

<sup>3</sup> Басыров Р. Р., Паршин К. А. Анализ защищённости электронных документов в системах ЭДО [Электронный ресурс] — Режим доступа — URL: <https://elar.urfu.ru/handle/10995/36239> (Дата обращения: 14.04.2026)

<sup>4</sup> Системы электронного документооборота [Электронный ресурс] — Режим доступа — URL: <https://www.sites.google.com/site/upravlenieznaniami/tehnologii> [upravlenia-znaniami/sistemy-elektronnogo-dokumentoborota](https://www.sites.google.com/site/upravleniaznaniami/sistemy-elektronnogo-dokumentoborota) (Дата обращения: 14.04.2026)

использованием сертифицированных криптографических инструментов; внедрение двухфакторной аутентификации для доступа к корпоративным сервисам.

Внедрение эффективной системы информационной безопасности и защиты персональных данных в коммерческой деятельности требует многостороннего подхода, охватывающего правовые, организационные, технические и физические аспекты.

Оптимизация финансовых рисков, связанных с утечками данных, кибератаками и незапланированными простоями, является первостепенной задачей. Соблюдение актуальных законов, таких как Федеральный закон «О персональных данных» от 27 июля 2006 № 152-ФЗ<sup>6</sup> и Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ,<sup>7</sup> позволяет избежать значительных штрафных санкций. Демонстрация надежных мер защиты конфиденциальной информации укрепляет доверие со стороны клиентов и партнеров, что, в свою очередь, способствует росту репутации компании. Внедрение комплексных систем безопасности повышает устойчивость бизнес-операций перед лицом киберугроз и технических сбоев. Кроме того, формирование имиджа и технологической инфраструктуры, ориентированной на безопасность, создает значительное конкурентное преимущество, привлекая как инвесторов, так и новых клиентов.

Для достижения наилучших результатов, предпринимаемые меры по обеспечению безопасности должны постоянно обновляться, отражая изменения в ландшафте угроз, нормативно-правовых актах и технологических инновациях. Для проведения независимых аудитов, разработки архитектуры и

---

<sup>6</sup> Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. №31. Ст. 3452.

<sup>7</sup> Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. №31. Ст. 3448.

поддержания эффективности системы защиты крайне полезным является привлечение экспертов в области информационной безопасности.

Таким образом, информационная безопасность является неотъемлемой частью эффективной деятельности организации, предотвращая ущерб коммерческой деятельности, конкурентоспособности и достижению стратегических целей. Системы электронного документооборота играют ключевую роль в обеспечении должного уровня информационной безопасности, автоматизируя делопроизводство, повышая исполнительскую дисциплину и ускоряя документопотоки.

#### **Использованные источники:**

1. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов н/Д: Феникс, 2010. — 324 с.
2. Международный научный журнал «ВЕСТНИК НАУКИ» № 11 (92) Том 3. 2025 г. — 915 - 916 с.
3. Системы электронного документооборота [Электронный ресурс] — Режим доступа — URL:[https://www.sites.google.com/site/upravlenieznaniami/tehnologii\\_upravleniaznaniami/sistemy-elektronnogo-dokumentoorota](https://www.sites.google.com/site/upravlenieznaniami/tehnologii_upravleniaznaniami/sistemy-elektronnogo-dokumentoorota) (Дата обращения: 14.04.2026)
4. Басыров Р.Р., Паршин К. А. Анализ защищённости электронных документов в системах ЭДО [Электронный ресурс] — Режим доступа — URL: <https://elar.urfu.ru/handle/10995/36239> (Дата обращения: 14.04.2026)
5. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. №31. Ст. 3452.
6. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. №31. Ст. 3448.