УДК528.71

И. С. Кажикин[1], М. И. Сидельников[1], П. Л. Солеева[1]✉

Анализ требований к обработке информации в автоматизированных информационных системах

[1]Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация
e-mail: psoleeva@mail.ru

Аннотация. В современном мире информационные системы играют ключевую роль в деятельности организаций всех уровней и секторов. Они становятся основой для эффективного управления, анализа данных и принятия обоснованных решений. С ростом технологий и увеличением объемов обрабатываемых данных вопросы безопасности и эффективности информационных систем становятся все более актуальными. В условиях цифровой трансформации, когда информация становится одним из самых ценных ресурсов, правильная организация и защита информационных систем не только обеспечивают конкурентные преимущества, но и являются важнейшим фактором для поддержания стабильности и безопасности общества и экономики.

Ключевые слова: информация, информационные системы, информационная безопасность

I. S. Kazhikin[1], M. I. Sidelnikov[1], P. L. Soleeva[1]✉

Analysis of information processing requirements in automated information systems

[1]Siberian State University of Telecommunication and Information Science,
Novosibirsk, Russian Federation
e-mail: psoleeva@mail.ru

Abstract. In the modern world, information systems play a key role in the activities of organizations at all levels and sectors. They become the basis for effective management, data analysis, and informed decision-making. With the growth of technology and the increase in the volume of data processed, the issues of security and efficiency of information systems are becoming more relevant. In the context of digital transformation, when information is becoming one of the most valuable resources, proper organization and protection of information systems not only provide competitive advantages, but are also an essential factor for maintaining the stability and security of society and the economy.

Keywords: information, information systems, information security

Введение

Современные информационные системы (далее – ИС) сталкиваются с множеством вызовов, включая киберугрозы, утечки данных и нарушения конфиденциальности. Эти угрозы могут иметь серьезные последствия, как для отдельных организаций, так и для всей инфраструктуры страны. Поэтому разработка и внедрение эффективных мер по защите ИС становится приоритетной задачей для бизнеса и государственных учреждений.

Обсуждение

В этой статье рассмотрены основные требования и положения, относящиеся к ИС, включая их классификацию и требования к их безопасности.

Актуальность этой темы обусловлена необходимостью постоянного совершенствования ИС для соответствия современным вызовам и стандартам безопасности. В условиях глобализации и цифровизации, организации должны быть готовы к быстрому реагированию на новые угрозы и изменения в законодательстве, что требует гибкости и инновационного подхода к управлению информационными ресурсами.

ИС – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Главным объектом защиты в ИС является обрабатываемая в ней информация.

Информация рассматривается как важный инструмент для выявления и анализа социальных и экономических тенденций, что способствует принятию обоснованных решений на уровне общества и государственных структур.

Для обеспечения защиты информации, содержащейся в ИС, оператором, согласно №149-ФЗ принимаются организационные и технические меры.

Организационные меры защиты ИС – это набор процедур, политик, практик и правил, которые внедряются в организации для обеспечения безопасности информации.

Они определяют общую стратегию защиты, а технические меры обеспечивают реализацию конкретных мероприятий, необходимых для достижения поставленных целей.

Меры защиты информации можно классифицировать по-разному, к примеру: по типу ИС, по способам обработки в ней информации, по уровням значимости.

Таким образом, в соответствии с установленным порядком Правительство РФ и регулирующие органы устанавливают необходимые требования и меры [1–8].

Рассмотрим свойства ИС. Их понимание критически важно для принятия обоснованных управленческих решений. Это знание позволяет оценивать возможности системы в контексте бизнес-задач и принимать решения о внедрении, обновлении или интеграции с другими системами, включая обеспечение информационной безопасности:

– любые ИС подлежат аналитическому, проектному и управленческому анализу на основе принципов системного подхода;

– ИС характеризуются непрерывным развитием и адаптацией к внешним изменениям;

– системный подход является обязательным методологическим инструментом при проектировании ИС;

– основной результат функционирования ИС заключается в генерации информации, используемой для принятия управленческих решений;

– ИС могут быть определены как человеко-машинные комплексы, предназначенные для обработки и передачи данных.

Никто не поспорит, что в условиях современного мира ИС занимают центральное место в деятельности организаций различных размеров и секторов. С ростом технологий и увеличением объемов, обрабатываемых данных, вопрос об эффективности ИС становится критически важным для достижения конкурентных преимуществ.

ИС можно классифицировать по разным критериям, к примеру: по сфере применения, по масштабам применения, по способам и методам обработки информации, по характеру обрабатываемой информации, по владельцу и т.п.

Рассмотрим классификацию ИС по признаку владения данными:

– государственные ИС (далее – ГИС);

– муниципальные ИС (далее – МИС);

– иные ИС.

Требования к организации защиты информации, содержащейся в ИС установлены Приказом ФСТЭК России от 11.02.2013 №17.

Защита информации в ИС является неотъемлемой частью процессов ее разработки и эксплуатации. Она осуществляется на всех этапах: от создания до вывода из эксплуатации с применением организационных и технических мер, направленных на выявление и нейтрализацию угроз безопасности информации. Эти угрозы могут быть как внешними, так и внутренними, включая кибератаки, ошибки сотрудников, уязвимости программного обеспечения и физические риски. Меры защиты формируют систему (подсистему) защиты информации, которая обеспечивает блокирование потенциальных рисков, угрожающих безопасности данных в ИС.

Под иными ИС понимаются, например, локальные информационные системы.

В зависимости от технологий, состава и характеристик технических средств ИС, а также опасности реализации угроз безопасности информации и наступления последствий в результате несанкционированного или случайного доступа можно выделить следующие типы ИС:

– автоматизированные рабочие места, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

– автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

– локальные ИС, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

– локальные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

– распределенные ИС, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

– распределенные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Значимость обрабатываемой информации ИС определяет системы, принадлежащие субъектам Критическая информационная инфраструктура (Далее – КИИ).

КИИ включает объекты, которые имеют важное значение для функционирования общества и экономики. К таким объектам относятся ИС, информационно-телекоммуникационные сети и автоматизированные системы управления. Эти элементы, а также сети электросвязи, обеспечивают взаимодействие между различными компонентами инфраструктуры, что является ключевым для обеспечения безопасности и стабильности.

Регулирование функционирования объектов КИИ осуществляется посредством ФЗ РФ от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказа ФСТЭК № 17 от 11.01.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и т.п.

Рассмотрим ИС в зависимости от обрабатываемой в них информации, а именно: коммерческая тайна, служебная тайна, персональные данные и т.п.

Необходимость создания автоматизированных систем обработки ПДн предусмотрена ФЗ РФ от 27.07.2006 № 152 «О персональных данных» (далее – ФЗ РФ №152-ФЗ). Требования к защите обрабатываемой в них информации утверждены Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Далее – ПП РФ № 1119).

В ПП РФ № 1119 рассматривается несколько различных ИС, например:

– ИС обрабатывает специальные категории персональных данных, если в ней содержатся данные о расовой или национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья и интимной жизни субъектов;

– ИС обрабатывает биометрические данные, если в ней хранятся индивидуальные сведения о физиологических и биологических характеристиках человека, которые позволяют установить его личность;

– ИС обрабатывает о персональные данные, находящиеся в общем доступе, если эти данные получены исключительно из свободных источников, созданных в соответствии с законодательством о персональных данных;

– ИС обрабатывает и другие категории персональных данных, если в ней не содержатся данные, указанные в первых трех пунктах;

– ИС обрабатывает персональные данные сотрудников оператора, если в ней хранятся только данные этих сотрудников, иначе система будет обрабатывать данные субъектов, не являющихся сотрудниками оператора.

ГИС создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

Информация, содержащаяся в ГИС, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламен-

тирующим функционирование ГИС, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной ИС, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

При взаимодействии различных ИС должны применяться комплексные организационные и технические меры безопасности, предусмотренные частью 4 статьи 19 ФЗ РФ №152-ФЗ. В частности, обязательно использование шифровальных средств, указанных в пункте 5 части 2 статьи 6 этого закона, либо иных сертифицированных средств криптографической защиты, обеспечивающих защиту персональных данных от угроз, установленных для государственных органов, органов местного самоуправления.

Безопасность персональных данных при их обработке в ИС обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 ФЗ РФ №152-ФЗ.

Федеральные и региональные органы власти, Банк России и другие государственные структуры в рамках своих полномочий принимают нормативные акты, которые определяют актуальные угрозы безопасности. Эти угрозы учитывают особенности данных, методы их обработки и специфику деятельности организаций.

К основным угрозам относятся несанкционированный доступ, утечка информации через технические каналы, внедрение вредоносного ПО и специальные воздействия на системы. Угрозы могут исходить как от внутренних пользователей, так и от внешних злоумышленников, и включают случайные ошибки, технические сбои и преднамеренные действия.

В Приказе ФСТЭК РФ от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждается комплекс различных мер для того, чтобы защитить персональных данных, хранящиеся в ИС.

Заключение

Вся информация, содержащаяся в ГИС, является официальной и должна быть достоверной и актуальной, что возлагает на государственные органы ответственность за ее защиту от неправомерного доступа и других угроз. В отличие от этого, ИСПДн сосредоточены на обработке персональных данных, что требует соблюдения более строгих норм, установленных ФЗ РФ №152-ФЗ, который регулирует принципы обработки, конфиденциальности и права субъектов на доступ и исправление данных. Важным аспектом является то, что ИСПДн подлежат классификации в соответствии с приказами ФСТЭК и другими регулирующими органами, что позволяет адаптировать меры защиты к специфике данных и угрозам. К основным угрозам для ИСПДн относятся несанкционированный доступ, утечка информации и внедрение вредоносного ПО, что требует от организаций

внедрения комплексных мер безопасности, включая антивирусную защиту и управление доступом. В то же время, для биометрических ГИС, согласно ФЗ РФ №572-ФЗ, предусмотрены дополнительные требования к безопасности, включая использование сертифицированных средств криптографической защиты.

В современных условиях цифровой трансформации информационные системы являются фундаментом эффективного управления и принятия решений в организациях. Их безопасность и эффективность требуют комплексного подхода, включающего организационные и технические меры, соответствующие законодательству и особенностям обрабатываемой информации. Только такой подход обеспечивает защиту данных, устойчивость инфраструктуры и конкурентные преимущества, что важно для стабильности общества и экономики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Законы. Об информации, информационных техно-логиях и о защите информации : Федер. закон N 149-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. : послед. ред. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.04.2025). Режим доступа: для любых пользователей.
2. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон N 187-ФЗ : принят Государственной Думой 12 июля 2017 г. : одобрен Советом Федерации 19 июля 2017 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 14.04.2025). Режим доступа: для любых пользователей.
3. Российская Федерация. Законы. О персональных данных : Федер. закон N 152-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 31.03.2025). Режим доступа: для любых пользователей.
4. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК РФ от 11.02.2013 г. N 17 // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения 09.04.2025).
5. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК от 15.02.2008 г. // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g (дата обращения 06.04.2025).
6. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК от 18.02.2013 г. N 21 // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 20.04.2025).
7. Российская Федерация. Правительство Российской Федерации. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ №1119 от 01.11.2012 г. // Правительство

Российской Федерации : офиц. сайт. URL: http://government.ru/docs/all/84743/ (дата обращения 18.04.2025).

8. Российская Федерация. Законы. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федер. закон N 572-ФЗ : принят Государственной Думой 21 декабря 2022 г. : одобрен Советом Федерации 23 декабря 2022 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 24.04.2025). Режим доступа: для любых пользователей.