

А. Я. Маршинина¹✉, В. В. Селифанов¹

Проблемные аспекты разработки и внедрения системы управления информационной безопасностью в IT-компаниях

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: marshinina-a@mail.ru

Аннотация. В статье рассматриваются проблемные аспекты разработки и внедрения системы управления информационной безопасностью в IT-компаниях. Основной проблемой исследования является противоречие между требованиями информационной безопасности и высокой скоростью изменения IT-среды. Целью работы является выявление ключевых организационных, технологических, экономических и кадровых барьеров при внедрении системы управления информационной безопасностью в IT-компанию. В качестве основных методов исследования использованы системный и сравнительный анализ, анализ нормативных документов и обобщение практического опыта внедрения системы управления информационной безопасностью в IT-среде. В результате исследования установлено, что ключевыми проблемами внедрения системы управления информационной безопасностью является низкий уровень интеграции безопасности в процесс разработки, низкая автоматизация контрольных процедур, дефицит квалифицированных кадров и сложности адаптации международных стандартов к динамической IT-среде. Также было установлено, что наиболее эффективным подходом является переход к модели непрерывного обеспечения безопасности, основанной на принципах DevSecOps. Основной вывод работы заключается в том, что успешное внедрение системы управления информационной безопасностью в IT-компанию возможно только при комплексной интеграции безопасности во все процессы разработки, эксплуатации и управления инфраструктурой компании с переходом к гибким и автоматизированным моделям.

Ключевые слова: система управления информационной безопасностью, информационная безопасность, информационные технологии, IT-компания, DevSecOps, кибербезопасность

A. Y. Marshinina¹✉, V. V. Selifanov¹

Problematic Aspects of Developing and Implementing of Information Security Management System Processes in IT Company

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: marshinina-a@mail.ru

Abstract. The article discusses the problematic aspects of developing and implementing an information security management system in IT companies. The main research problem is the contradiction between the requirements of information security and the high rate of change in the IT environment. The goal of the study is to identify the key organizational, technological, economic, and personnel barriers to implementing an information security management system in an IT company. The main research methods used are system and comparative analysis, analysis of regulatory documents, and generalization of practical experience in implementing an information security management system in the IT environment. The study found that the key challenges in implementing an information security management system are the low level of security integration into the development process, the low level of automation of control procedures, the shortage of qualified

personnel, and the difficulties in adapting international standards to a dynamic IT environment. The study also found that the most effective approach is to transition to a continuous security assurance model.

Keywords: information security management system, information security, information technologies, IT companies, DevSecOps, cybersecurity

Введение

В условиях стремительного развития цифровых технологий информационная безопасность становится одним из основных факторов устойчивого функционирования компании. Большие объемы обрабатываемых данных, рост распределенных систем и усиление зависимости бизнеса от IT сферы обуславливает необходимость системного подхода к обеспечению защиты информации в IT-компаниях.

Именно внедрение системы управления информационной безопасностью (здесь и далее СУИБ) позволит сделать обеспечение безопасности системной. СУИБ основаны на международных стандартах и лучших практиках и позволяют сделать информационную безопасность более эффективной.

Согласно стандарту ГОСТ Р ИСО/МЭК 27000-2021, СУИБ является частью общей системы менеджмента организации, основанной на подходе управления рисками. Основной ее целью является создание, внедрение, использование, мониторинг и постоянное улучшение информационной безопасности предприятия [1]. В ГОСТ Р ИСО/МЭК 27001-2021 закреплены основные требования к таким системам. Они включают в себя обязательное документирование процессов, оценку рисков и внедрение определенных мер защиты [2].

Актуальность исследования обусловлена тем, что, несмотря на наличие нормативной базы и большого количества методических материалов, процесс разработки и внедрения СУИБ в IT-компаниях связан с некоторыми сложностями. Эти компании существуют в условиях высоких скоростей изменений. Релизы программного обеспечения могут происходить многократно за сутки, инфраструктура использует подходы Infrastructure as Code, а команды разработки работают по привычным методологиям. В таких условиях классические подходы к внедрению СУИБ часто оказываются недостаточно эффективными.

Исследования А. Д. Назарова указывают на рост числа киберугроз в условиях цифровой трансформации, что требует от организации более гибких и адаптивных механизмов защиты [3].

Н. Ю. Изварина отмечает необходимость комплексного подхода к экономической безопасности, частью которой является информационная безопасность [4].

А. Д. Георгиевский и Ю. Ю. Черемухина также подчеркивают, что внедрение СУИБ в информационную безопасность постоянно необходимо актуализировать под существующие условия в компании [5].

Несмотря на большое количество исследований, остаются незакрытыми вопросы, связанные с применением стандартов СУИБ в IT-компаниях. Слабо рассмотрена интеграция систем в гибкие методологии разработки и оценка эффек-

тивности такого внедрения. Помимо этого, все еще недостаточно изучены организационные барьеры, которые возникают в процессе внедрения СУИБ в организациях.

В качестве цели данного исследования выбран анализ проблемных аспектов разработки и внедрения СУИБ в ИТ-компаниях и формирование основных рекомендаций по устранению с учетом их специфики. Для достижения поставленной цели будут решаться следующие задачи:

- провести анализ существующих подходов к построению СУИБ;
- выявить основные проблемы внедрения СУИБ;
- предложить практические решения, которые будут обеспечивать эффективность функционирования СУИБ.

Методы и материалы

В процессе исследования использовался комплекс научных методов, позволяющих всесторонне проанализировать обозначенную проблему. Проводился анализ нормативно-правовой базы, позволяющий определить основные требования к построению СУИБ. Благодаря сравнительному анализу научных публикаций, были выявлены общие тенденции различия в подходах к внедрению СУИБ. Через системный анализ была рассмотрена СУИБ как комплексная система, включающая организационный, технический и управленческие аспекты. Благодаря этому выявлена взаимосвязь между различными компонентами системы и определены основные точки возникновения проблем.

Были проанализированы национальные стандарты РФ, связанные с СУИБ - ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27005-2010.

Помимо этого, использовался метод кейс-стади, демонстрирующий практический опыт внедрения СУИБ в ИТ-компаниях.

Результаты

В ходе проведенного исследования были обозначены основные группы проблем, которые возникают при разработке и внедрении СУИБ в ИТ-компаниях.

К числу наиболее значимых относятся организационные проблемы. Во многих компаниях наблюдается недостаточно вовлеченность в процесс как руководства, так и сотрудников. Этот фактор делает внедрение СУИБ формальным процессом. Система существует лишь на уровне документации, не отражая реальные бизнес-процессы. Также наблюдается сопротивление со стороны персонала, связанное с увеличением количества регламентов и ограничений. Команды разработки зачастую привыкли работать по Agile методологиям и ориентированы на быстрый запуск функционала [6]. В то время как СУИБ требует формализации процессов и соблюдение определенных регламентов и времени. Согласно статистике, внедрение СУИБ в компании требует от 12–18 месяцев [7]. Это приводит к сопротивлению со стороны сотрудников и попыткам обхода мер безопасности. Также было установлено, что большая часть проблем возникает на этапе интеграции уже в существующие бизнес-процессы. Компании необходимо перестра-

ивать процессы, что требует дополнительных ресурсов и времени. И этот момент также может снова вызвать сопротивление со стороны персонала.

Также возникают проблемы при интеграции СУИБ в текущие DevOps-процессы. ИТ-компании функционируют на основе DevSecOps подхода, который предполагает внедрение механизма безопасности на всех этапах жизненного цикла разработки [6].

Наглядно представлено на рисунке (Рис. 1).



Рис. 1. Интеграция СУИБ в жизненный цикл разработки

Но на практике этот процесс сталкивается с определенными трудностями:

- внедрение автоматизированных инструментов онлайн анализа кода (SAST, DAST);
- обеспечение безопасности зависимостей;
- защита CI/CD-пайплайнов от компрометации;
- управление «секретами» (ключами, токенами, паролями) [8].

Технологические проблемы проявляются в момент интеграции СУИБ в уже существующую инфраструктуру ИТ. В разных ИТ-компаниях используются разные программные решения, облачные сервисы и распределенные системы, которые не позволяют быстро внедрять единые стандарты безопасности. Дополнением выступает и быстрое развитие технологий, требующих постоянного обновления средств защиты.

В ряде ИТ-компаний применяется модель разделения ответственности, при которой функции по обеспечению информационной безопасности распределяются между облачным провайдером и самой организацией. В таком случае особенно важно определить зоны ответственности каждой стороны и выстроить понятную систему контроля доступа.

Серьезным ограничением при внедрении СУИБ остается экономический фактор. Затраты связаны не только с внедрением самой системы, но и с ее встраиванием в уже действующие автоматизированные процессы компании. Это, как правило, увеличивает общий объем инвестиций, поскольку дополнительные ресурсы требуются также на обучение сотрудников и адаптацию рабочих процессов.

Также имеют место быть и методологические проблемы. Они обусловлены тем, что международные стандарты в области информационной безопасности не всегда в полной мере учитывают особенности деятельности ИТ-компаний. Обычно такие стандарты разрабатываются как универсальные и поэтому слабо соотносятся с гибкими подходами к разработке, включая Agile и DevOps. Таким образом, компаниям необходимо самостоятельно подстраивать требования, что значительно увеличивает сложность внедрения [10].

Еще одной существенной проблемой является дефицит квалифицированных специалистов, способных участвовать во внедрении и сопровождении СУИБ. Без автоматизации процессов, выращивания кадров внутри компании и упрощения регуляций внедрение СУИБ рискует остаться формальным: компания тратит бюджеты, но остается уязвимой к реальным угрозам из-за нехватки экспертизы. Согласно статистическим данным, в 2025 году 88% компаний столкнулись с нехваткой специалистов в сфере ИБ [11]. При этом спрос на квалифицированные кадры продолжает существенно опережать предложение, что ведет к росту расходов на их поиск, привлечение и удержание сотрудников.

Обсуждение

Полученные результаты подтверждают выводы исследователей о том, что внедрение СУИБ является важным, сложным и многоэтапным процессом.

Так А. Д. Назарова подчеркивает, что в цифровой трансформации возрастает значение гибкости и адаптивности систем информационной безопасности [3]. Это согласуется с обозначенными в ходе исследования проблемами, связанными с адаптацией стандартов.

В сравнении с работами авторов, которые ориентированы на экономическую безопасность организации, было выявлено, что в ИТ-компаниях на первый план выходят технологические и организационные аспекты.

В случаях, когда внедрение новой системы воспринимается как препятствие и будет обходиться специалистами, она не будет эффективно реализована. Внедрение различных концепций требует значительных изменений в организационной культуре и в процессах в целом.

Также важным является использование инструментов автоматического мониторинга и реагирования для обеспечения безопасности в условиях высокой скорости изменения ИТ-сферы.

Заключение

Проведенное исследование показало, что разработка и внедрение СУИБ в ИТ-компаниях сопровождаются рядом как объективных, так и управленческих

трудностей, связанных со спецификой применяемых стандартных моделей, особенностями внутренних информационных систем и условиями функционирования современной ИТ-среды

Основными проблемами являются конфликт между необходимостью высокой скорости разработки и эксплуатации решений и соблюдением требований информационной безопасности, сложности интеграции СУИБ в DevOps процессы, риски, связанные с облачными инфраструктурами, и нехватка квалифицированных специалистов. Для повышения эффективности СУИБ в ИТ-компаниях рекомендуется внедрять принципы DevSecOps, автоматизировать процессы контроля безопасности, интегрировать инструменты безопасности CI/CD, развивать культуру информационной безопасности в командах разработки и совершенствовать механизмы управления доступами и защиту конфиденциальных данных. Для минимизации указанных проблем необходимо сочетать стратегический подход (дорожная карта, цикл PDCA, управление рисками) с технической согласованностью решений и регулярной оценкой эффективности системы через аудиты и метрики.

Перспективным направлением дальнейших исследований видятся разработка адаптивных модулей СУИБ, предназначенных для динамично изменяющихся сред, в которых функционируют ИТ-компании.

Таким образом, успешное внедрение СУИБ в ИТ-компании возможно только при переходе от преимущественно статических моделей управления безопасностью к гибким, интегрированным и автоматизированным подходам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. - М.: Российский институт стандартизации, 2021.
2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. - М.: Российский институт стандартизации, 2021. – С. 1-8.
3. Назарова А. Д. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации / Назарова А. Д. // Столыпинский вестник. -2023. – №5. – С. 2212-2214.
4. Изварина Н. Ю. Использование комплексной системы экономической безопасности в практической работе компании / Н. Ю. Изварина, А. Ю. Серикова, А. А. Уварова, А. Г. Голубова // Экономика и бизнес: теория и практика. 2022. – №7 (89). – С. 82-85.
5. Георгиевский А. Д., Черемухина Ю. Ю. Система обеспечения информационной безопасности и внедрение механизмов управления // Компетентность / Competency (Russia). 2025. – № 10.
6. Построение СУИБ: С чего начать? – URL: <https://habr.com/ru/artides/233315/> (дата обращения 18.04.2026). – Текст: электронный.
7. ISO 27001 Framework: Полное руководство + Практические советы. – URL: <https://foundor.ai/ru/blog/iso-27001> (дата обращения 18.04.2026). – Текст: электронный.
8. Ким М. Е. Организация системы управления информационной безопасностью на предприятии / М. Е. Ким, С. Г. Самохвалова // Вестник Амурского государственного университета. Серия: Гуманитарные науки. 2025. – С. 101-105.

9. Дербин Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. – Москва : ИНФРА-М, 2024. – 267 с.

10. Платонов В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. - Москва ; Вологда : Инфра-Инженерия, 2024. – 140 с.

11. SC2 Cybersecurity Workforce Study 2025. – URL: <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study> (дата обращения 18.04.2026). – Текст: электронный.

© А. Я. Мариинина, В. В. Селифанов, 2026