УДК: 004.056.53

Екимов Дмитрий Александрович
Ученая степень - Студент магистратуры
Кафедра - Безопасность в инфокоммуникационных технологиях и системах связи
Название ВУЗа - Сибирский государственный университет телекоммуникаций и информатики
Научный руководитель: Попков Г. В.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ РИСКАМИ

Аннотация: В статье рассматривается аудит информационной безопасности как инструмент управления рисками. На основе анализа научной и нормативной литературы раскрываются сущность и цели аудита ИБ, его виды и классификация, а также роль в выявлении и оценке информационных рисков. Показано, что аудит ИБ выполняет как контрольную функцию соответствия нормативным требованиям, так и управленческую функцию, обеспечивая интеграцию результатов в систему риск-ориентированного управления организацией. Цель исследования — определить возможности применения аудита информационной безопасности для системной оценки, снижения и управления информационными рисками. Полученные выводы подчеркивают практическую значимость аудита как инструмента повышения устойчивости организаций к информационным угрозам и оптимизации мер защиты информации.

Ключевые слова: аудит, цифровизация, информационная безопасность, риск, безопасность.

В условиях цифровизации информационные ресурсы становятся ключевым активом организаций, а рост числа киберугроз увеличивает риски нарушения конфиденциальности, целостности и доступности данных. Аудит информационной безопасности позволяет объективно оценить текущее состояние защиты, выявить уязвимости и определить уровень рисков. Однако в практике многих организаций аудит рассматривается лишь как формальная проверка соответствия требованиям, без интеграции в систему управления рисками. Это снижает эффективность мер защиты и делает организацию уязвимой перед современными угрозами. Поэтому исследование аудита ИБ как инструмента управления рисками является актуальным с точки зрения как науки, так и практики.

Аудит информационной безопасности представляет собой систематический и документированный процесс получения и анализа информации о состоянии защиты информационных ресурсов организации. Его основная цель заключается в оценке эффективности применяемых мер безопасности, а также в выявлении несоответствий, уязвимостей и потенциальных источников информационных рисков. В отличие от разовых проверок, аудит ИБ носит комплексный характер и охватывает как технические, так и организационные аспекты защиты информации.

Сущность аудита информационной безопасности заключается в формировании объективного представления о степени защищённости информационной системы и её способности противостоять актуальным угрозам. В ходе аудита анализируются политики и процедуры безопасности, архитектура информационных систем, уровень осведомлённости персонала, а также соответствие установленным требованиям и стандартам. Полученные результаты

служат информационной основой для принятия управленческих решений в области обеспечения информационной безопасности.

Таким образом, аудит информационной безопасности следует рассматривать не только как инструмент контроля, но и как элемент системы управления, направленный на повышение устойчивости организации к информационным рискам и обеспечение непрерывности её деятельности.

Аудит информационной безопасности выполняет ряд взаимосвязанных функций, направленных на повышение уровня защищённости информационных ресурсов организации. В рамках аудита осуществляется оценка соответствия существующих мер безопасности установленным требованиям, анализ эффективности применяемых технических и организационных решений, а также выявление факторов, способствующих возникновению информационных рисков. Особенностью аудита информационной безопасности является его комплексный характер, предполагающий рассмотрение системы защиты информации как единого целого, а не совокупности отдельных средств и процедур.

В зависимости от целей и условий проведения аудит информационной безопасности может принимать различные формы. Он может осуществляться как силами самой организации, так и с привлечением внешних специалистов, что позволяет обеспечить различный уровень независимости и глубины анализа. Кроме того, аудит может быть ориентирован на проверку соответствия нормативным требованиям либо на оценку реальной эффективности системы защиты информации. Выбор конкретного подхода определяется уровнем зрелости системы управления информационной безопасностью и характером информационных рисков, с которыми сталкивается организация.

Важную роль в процессе аудита информационной безопасности играет нормативно-правовая и методическая база. Международные и национальные стандарты в области информационной безопасности формируют единые требования к организации системы защиты информации и проведению оценочных мероприятий. Их использование в аудиторской практике позволяет обеспечить сопоставимость результатов, повысить объективность выводов и создать основу для внедрения риск-ориентированного подхода к управлению информационной безопасностью.

Рассмотрение информационной безопасности в контексте управления рисками предполагает выявление потенциальных угроз, анализ уязвимостей и оценку возможных последствий реализации негативных сценариев. Информационные риски могут быть обусловлены как техническими сбоями и недостатками программно-аппаратных средств, так и организационными факторами, связанными с человеческим фактором и несовершенством внутренних регламентов. Реализация таких рисков способна оказывать существенное влияние на финансовые показатели организации, её деловую репутацию и непрерывность бизнес-процессов.

В системе управления организацией аудит информационной безопасности выступает инструментом, обеспечивающим информационную поддержку процесса принятия управленческих решений. Результаты аудита позволяют не только зафиксировать текущее состояние системы защиты, но и определить приоритетные направления её развития с учётом уровня выявленных рисков. На основе полученных данных формируются рекомендации по снижению вероятности возникновения инцидентов информационной безопасности и минимизации возможного ущерба.

Итак, аудит информационной безопасности следует рассматривать как важный элемент риск-ориентированной модели управления, интегрированный в общую систему менеджмента организации. Его применение способствует переходу от формального соблюдения требований к осознанному управлению информационными рисками, что приобретает особую значимость в условиях усложнения информационной среды и роста числа угроз.

Аудит информационной безопасности рассматривается в научной и практической литературе как систематизированная, независимая и документированная процедура, предназначенная для оценки соответствия мер защиты установленным критериям и стандартам, а также для получения объективной информации о текущем состоянии системы защиты информации организации. Важность этой процедуры заключается в способности не только выявлять уязвимости, но и обеспечивать основную информацию для анализа рисков, что делает аудит одним из ключевых компонентов риск-ориентированного подхода к управлению ИБ — по сути, инструментом, связывающим оценку риска с практикой управления им .

Важным элементом современной практики является интеграция аудита информационной безопасности в систему менеджмента информационной безопасности (СМИБ), в которой управление рисками выступает центральным процессом. Международный стандарт ISO/IEC 27001, являющийся основой СМИБ, прямо включает в себя требования по выявлению, оценке и обработке рисков информационной безопасности, что делает аудит неотъемлемой частью управления рисками и обеспечению защиты активов организации . Подобный подход отражает эволюцию ИБ-аудита от формального контроля к активному инструменту

управления — с фокусом на оценке угроз, уязвимостей и последствий их реализации.

Практические исследования также подтверждают, что применение риск-ориентированного подхода в аудите информационной безопасности повышает эффективность оценки защищённости организации. К примеру, в отечественной научной литературе предлагается методика, основанная на теории управления рисками, которая позволяет не только выявлять слабые места в системе защиты, но и формировать план мероприятий по снижению рисков, улучшая взаимодействие между подразделениями, ответственными за безопасность и управление рисками .

Важно отметить, что аудит ИБ может выполняться в различных формах, включая внутренний и внешний аудит, а также аудит на соответствие стандартам, что расширяет возможности его применения в управлении рисками. Внутренний аудит предоставляет регулярную информацию для менеджмента о рисках и эффективности мер защиты, а внешний аудит обеспечивает независимую оценку, востребованную для соответствия нормативным требованиям и для повышения доверия заинтересованных сторон .

Таким образом, аудит информационной безопасности выполняет двойную функцию: с одной стороны — он служит механизмом контроля соответствия установленным требованиям, а с другой — играет активную роль в выявлении, оценке и снижении рисков, что обеспечивает организацию важной информационной основой для принятия управленческих решений. Этот подход формирует предпосылки для перехода от изолированных процедур к интегрированной системе управления ИБ, ориентированной на

устойчивость организации в условиях динамичного развития угроз и технологической среды.

В ходе проведённого исследования был рассмотрен аудит информационной безопасности как один из ключевых инструментов управления рисками в деятельности современной организации. Установлено, что в условиях цифровизации и роста количества информационных угроз традиционные подходы к обеспечению информационной безопасности, основанные исключительно на формальном соблюдении требований, не обеспечивают достаточного уровня защищённости информационных ресурсов.

Показано, что аудит информационной безопасности позволяет получить системное представление о состоянии защиты информации, выявить уязвимости и определить уровень информационных рисков, влияющих на устойчивость бизнес-процессов. При этом наибольшую практическую ценность аудит приобретает в случае его интеграции в систему управления рисками и использования его результатов при принятии управленческих решений. Такой подход обеспечивает переход от реактивных мер реагирования к проактивному управлению угрозами и уязвимостями.

В результате анализа установлено, что риск-ориентированное применение аудита информационной безопасности способствует повышению эффективности системы менеджмента информационной безопасности, позволяет обоснованно определять приоритеты защитных мероприятий и оптимизировать использование ресурсов организации. Аудит в данном контексте выступает не только инструментом контроля, но и элементом стратегического управления, направленным на снижение вероятности реализации информационных рисков и минимизацию возможного ущерба.

Резюмируя вышесказанное можно отметить, что аудит информационной безопасности следует рассматривать как важный компонент комплексной системы управления рисками, обеспечивающий повышение уровня защищённости информационных активов и устойчивости деятельности организации в целом. Полученные выводы могут быть использованы в практической деятельности организаций при совершенствовании системы информационной безопасности, а также в дальнейших научных исследованиях, посвящённых развитию риск-ориентированных методов управления в сфере ИБ.

Список использованной литературы

1. Глыбовский П. А., Тимашов П. В., Чернышов В. И. Метод обеспечения и проведения внутреннего аудита информационной безопасности организаций на основе риск-ориентированного подхода // Проблемы информационной безопасности. Компьютерные системы. 2023. № 3. С. 09-24.
2. Павлов Е. О., Резниченко С. А. Организационно-правовые особенности аудита информационной безопасности в кредитных организациях Российской Федерации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 36-53.
3. Бакин И. Б., Ниязова К. Ш., Шведова С. М. Проблемы управления рисками в сфере информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 3. С. 49-60.

4. Козырь Н. С., Хализев В. Н. Оценка рисков и аудит информационной безопасности : учебник для вузов / М.: Юрайт, 2025.

5. Комплексный подход к управлению рисками информационной безопасности // Современные технологии и научно-технический прогресс. 2023. № 1. С. 101-102.

6. Халимов Ш. М., Селиверстова Н. С. Обзор рисков рынка кибербезопасности Российской Федерации // Вестник науки. 2025.

7. Википедия. Аудит информационной безопасности (описание сущности, целей и задач аудита ИБ) — электрон. ресурс: https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (дата обращения: 22.01.2026)