

Тема 5

Перспективы использования компьютерных технологий в организации внутреннего контроля

1. Автоматизация внутреннего контроля.
2. Требования к программному обеспечению внутреннего контроля.
3. План проведения внутреннего контроля.
4. Проверка полноты информации и внутреннего контроля.

1. Автоматизация внутреннего контроля

Автоматизация внутреннего контроля – это использование компьютерных программ и технологий, чтобы проверять работу организации без постоянного участия человека. Например, специальная программа может сама сверять данные в документах, следить за лимитами расходов или напоминать о сроках отчётности.

Главная цель автоматизации – сделать контроль быстрее, точнее и охватить больше операций. Вместо того чтобы человек вручную проверял 10–20 документов, программа может проанализировать тысячи за считанные минуты.

Автоматизация помогает:

- Снизить число ошибок: программы не устают и не отвлекаются.
- Экономить время: рутинные проверки выполняются автоматически.
- Повысить прозрачность: все действия фиксируются в системе, легко найти, кто и когда что делал.

- Соблюдать требования закона: например, для налогового мониторинга ФНС требует, чтобы компании использовали автоматизированные системы контроля.

Даже в небольших организациях уже есть элементы автоматизации:

- 1С:Бухгалтерия: программа сама проверяет, правильно ли заполнены реквизиты, не нарушены ли правила учёта. Если бухгалтер попытается провести операцию с ошибкой, система выдаст предупреждение.

- Банковские сервисы: когда компания платит поставщику, банк автоматически проверяет реквизиты и блокирует подозрительные платежи.

- Электронные таблицы (Excel): с помощью формул можно настроить проверку сумм, дат, других параметров. Например, если сумма платежа больше 100 тысяч рублей, ячейка автоматически окрашивается в жёлтый цвет – сигнал для дополнительной проверки.

Какие задачи можно автоматизировать:

- Сверка данных: программа сравнивает информацию из разных источников (например, накладные и записи в учётной системе) и отмечает расхождения.

- Контроль лимитов: если сотрудник пытается оформить заказ на сумму выше разрешённой, система блокирует операцию или отправляет запрос на согласование.

- Мониторинг сроков: автоматические напоминания о том, что пора сдать отчёт, оплатить счёт, провести инвентаризацию.

- Анализ рисков: сложные системы могут выявлять подозрительные операции (например, частые платежи одному и тому же контрагенту на грани лимита).

Для автоматизации используют разные программы и технологии:

- Учётные системы (1С, SAP): ведут учёт и одновременно контролируют правильность операций.

- RPA (роботизированная автоматизация процессов): «роботы» выполняют рутинные действия – переносят данные из одного документа в другой, формируют отчёты.

- BI-системы (Power BI, Tableau): собирают данные из разных источников и показывают их в виде наглядных графиков и диаграмм. Например, можно сразу увидеть, в каком месяце было больше всего ошибок в учёте.

- Простые скрипты и макросы: небольшие программы, которые автоматизируют действия в Excel или других приложениях.

Преимущества:

- Снижение ошибок на 30-70 % за счёт исключения человеческого фактора.

- Сокращение времени на рутинные проверки (например, закрытие отчётного периода ускоряется на 20-40 %).

- Повышение прозрачности для аудиторов и регуляторов.

- Возможность предиктивной аналитики: выявление рисков до их реализации.

Риски и ограничения:

- Высокие затраты на внедрение (особенно для комплексных систем типа GRC).

- Зависимость от качества исходных данных: «мусор на входе – мусор на выходе».

- Сопротивление сотрудников изменениям (страх потери контроля или рабочих мест).

- Риски информационной безопасности (утечки, сбои в работе систем).

2. Требования к программному обеспечению внутреннего контроля

Требования к программному обеспечению (ПО) внутреннего контроля — это набор условий, которые должны соблюдаться при разработке, внедрении и эксплуатации систем, обеспечивающих мониторинг, анализ и управление рисками в организации. Такие системы помогают автоматизировать контрольные процедуры, повысить достоверность данных и снизить риски ошибок или нарушений.

Функциональные требования. ПО должно реализовывать ключевые функции внутреннего контроля, такие как:

- настройка контрольных процедур (определение правил проверки операций, например, запрет проводок в закрытом периоде или обязательное двойное согласование крупных платежей);

- мониторинг в реальном времени по ключевым индикаторам риска (KRI) с оповещением ответственных лиц;

- сверка данных из разных источников (например, остатков на складах и в бухгалтерии);

- формирование отчётов для руководства, аудиторов и регуляторов (в том числе в форматах, требуемых ФНС для налогового мониторинга);

- управление рисками: ведение реестра рисков, назначение ответственных, контроль сроков устранения нарушений;

- контроль доступа с разграничением прав пользователей и журналированием действий.

Требования к обработке данных. ПО должно обеспечивать:

- полноту охвата – обработку 100% транзакций, а не выборочных данных;

- валидацию входных данных – проверку корректности реквизитов, форматов, ссылок на нормативные акты;

- обработку исключений – механизм для ручной проверки операций, которые система не может оценить автоматически (например, нестандартные договоры);

- резервное копирование и восстановление данных для защиты от потери информации при сбоях.

Нормативные и юридические требования. ПО должно соответствовать:

- ФЗ-152 «О персональных данных», если обрабатывает персональные данные (требования к шифрованию и анонимизации);

- требованиям ФНС для участников налогового мониторинга (возможность выгрузки данных в утверждённых форматах);
- стандартам ЦБ РФ для финансовых организаций (например, требования к контролю платёжных операций).

Технические требования. К ним относятся:

- производительность – обработка больших массивов данных без задержек;
- совместимость с актуальными версиями ОС, СУБД и браузеров;
- наличие API и открытых протоколов для интеграции с внешними сервисами (например, проверка контрагентов через API «СПАРК» или «Контур.Фокус»);
- локализация — интерфейс и документация на русском языке, поддержка российских стандартов (ОКПО, ОКТМО и др.).

Требования к безопасности. Включают:

- аутентификацию и авторизацию – многофакторную аутентификацию, ролевую модель доступа;
- шифрование данных при передаче (TLS) и хранении;
- журналирование всех действий пользователей и системных событий с возможностью аудита;
- защиту от несанкционированных изменений – механизмы контроля целостности конфигураций и алгоритмов проверки.

Требования к аналитике и отчётности. ПО должно предоставлять:

- гибкую настройку отчётов – возможность создавать шаблоны под нужды компании и регуляторов;
- визуализацию данных – дашборды с KPI и KRI (например, количество нарушений по типам, динамика рисков);
- предиктивную аналитику – использование ML-алгоритмов для прогнозирования рисков (например, выявление схем мошенничества);
- экспорт данных в форматы PDF, Excel, XML.

При выборе ПО для внутреннего контроля важно учитывать специфику организации, её масштабы и отраслевые особенности. Для малого бизнеса могут подойти модули 1С, для корпораций – решения уровня SAP GRC или специализированные GRC-платформы.

3. План проведения внутреннего контроля

План внутреннего контроля – это документ, в котором прописаны все предстоящие проверки внутри организации: что будут проверять, когда, кто отвечает и какими методами. Его составляют на год вперёд (годовой план), а потом уточняют ежемесячно.

Главная цель плана – организовать контроль системно, чтобы не упустить важные направления и не перегружать сотрудников частыми проверками.

В крупных организациях за план отвечает служба внутреннего контроля или внутренний аудитор. В небольших компаниях – главный бухгалтер, заместитель директора или другой уполномоченный сотрудник.

План обязательно утверждает руководитель организации. Без его подписи документ не имеет силы.

Этапы составления плана:

- Анализ рисков и «слабых мест». Нужно понять, где чаще всего бывают ошибки или злоупотребления. Например, в кассе, при закупках, при начислении зарплаты. Для этого изучают результаты прошлых проверок, жалобы, данные учёта.
- Определение объектов контроля. Что именно будем проверять: кассовые операции, расчёты с поставщиками, сохранность имущества, соблюдение инструкций и т. д.
- Выбор видов и форм контроля. Виды контроля бывают разные:

- Плановый – по утверждённому графику.
 - Внезапный (оперативный) – без предупреждения, чтобы проверить реальную ситуацию.
 - Тематический – проверка одной узкой темы (например, только командировочные расходы).
 - Комплексный – проверка сразу нескольких направлений.
- Назначение сроков. Проверки распределяют по месяцам так, чтобы они не совпадали и не мешали основной работе.
- Формирование рабочей группы. Определяют, кто будет проводить проверку: один сотрудник или группа специалистов.
- Определение методов проверки. Какие приёмы будут использовать проверяющие:
- инвентаризация (пересчёт имущества);
 - сверка документов;
 - опрос сотрудников;
 - анализ отчётов и т. д.
- Оформление документа. Готовый план записывают в таблицу или специальный бланк.

Структура типового плана (пример таблицы)

№ п/п	Объект контроля	Вид контроля	Срок проведения	Ответственные лица	Методы проверки
1	Кассовые операции	Плановый, тематический	10–15 марта	Главный бухгалтер, кассир	Инвентаризация кассы, сверка кассовой книги
2	Расчёты с поставщиками	Плановый, комплексный	20–25 апреля	Бухгалтер по расчётам, экономист	Сверка актов, анализ задолженности
3	Сохранность инвентаря	Внезапный	5 мая (без предупреждения)	Комиссия из 3 человек	Пересчёт инвентаря, сверка с карточками учёта

Как проходит проверка по плану:

1. Подготовительный этап. Проверяющие изучают нормативные акты, инструкции, прошлые отчёты. Готовят бланки для записей.
2. Основной этап. Непосредственно проверка: пересчёт, сверка, опрос. Всё фиксируют в рабочих документах (актах, ведомостях).
3. Заключительный этап. Составляют отчёт (справку) о результатах. Указывают выявленные нарушения, причины и предложения по исправлению. Отчёт передают руководителю.

По итогам проверки оформляют один из документов:

Акт – если найдены нарушения. В нём подробно описывают, что и где нарушено, на какую сумму, кто виноват.

Справка – если нарушений нет или они незначительные. Кратко фиксируют, что проверено и что в порядке.

Служебная записка – для оперативных сообщений руководству.

К акту или справке могут прилагать копии документов, фото, расчёты — всё, что подтверждает выводы проверяющих.

4. Проверка полноты информации и внутреннего контроля

Полнота информации – это требование, согласно которому все факты хозяйственной жизни организации должны быть зафиксированы в учёте и отчётности. Ни одна операция не должна «потеряться»: если товар поступил на склад, это должно быть отражено в документах; если деньги ушли поставщику, это должно быть записано в кассовой книге или банковской выписке.

Если информация неполная, руководство не сможет принимать верные управленческие решения, а организация рискует получить штраф от налоговой.

Проверка полноты нужна, чтобы:

- Не было «пропавших» операций: иногда документы забывают провести в учётной программе, и это искажает картину дел.

- Совпадали данные в разных источниках: например, количество товара по накладной должно совпадать с записью в складском журнале и в бухгалтерской программе.

- Отчётность была достоверной: перед сдачей отчётов в налоговую или перед годовой инвентаризацией нужно убедиться, что учтены все операции за период.

Основные методы проверки полноты информации

Сверка документов. Проверяющий берёт первичные документы (накладные, акты, кассовые ордера) и сравнивает их с записями в учётных регистрах (журналах, ведомостях, программе 1С). Задача – найти расхождения.

Встречная проверка. Если организация отправила счёт-фактуру клиенту, нужно убедиться, что клиент получил её и отразил в своём учёте. Это особенно важно для НДС.

Арифметическая проверка. Пересчёт сумм в документах и проверка итогов в ведомостях. Например, если в накладной 10 позиций, нужно сложить их стоимость и сравнить с итоговой суммой.

Проверка нумерации. Документы (особенно кассовые и банковские) должны идти подряд, без пропусков. Если в кассе были ордера № 101, 102, 104, но нет № 103 – это повод разобраться, куда он делся.

Инвентаризация. Пересчёт реальных активов (денег в кассе, товаров на складе) и сверка с учётными данными. Если по учёту на складе 100 стульев, а по факту 95 – информация неполная или неверная.

Практический пример: проверка полноты кассовых операций

Представим, что мы проверяем кассу магазина за неделю. Что делаем:

1. Берём все приходные и расходные кассовые ордера за неделю.
2. Сверяем их с записями в кассовой книге.
3. Проверяем нумерацию ордеров: нет ли пропусков.
4. Считаем итог по приходу и расходу в кассовой книге и сверяем с фактическим остатком денег в кассе.
5. Если есть расхождения – выясняем причину (например, забыли провести ордер или ошиблись в сумме).

Внутренний контроль – это не только проверка цифр, но и проверка того, как устроены процессы в организации. Чтобы понять, работает ли система контроля, проверяют:

- Наличие регламентов и инструкций. Должны быть документы, где написано: кто отвечает за каждый участок работы, какие правила нужно соблюдать.

– Разделение обязанностей. Например, кассир не должен сам подписывать расходные документы, а бухгалтер не должен иметь доступ к кассе. Это снижает риск злоупотреблений.

– Документооборот. Все документы должны оформляться вовремя и передаваться по назначению. Если накладные лежат на столе у кладовщика неделю и не попадают в бухгалтерию – система контроля нарушена.

– Результаты прошлых проверок. Если в прошлом году нашли нарушения, нужно проверить, устранены ли они сейчас.

Типичные ошибки, которые выявляет проверка

– Пропущенные документы: операция была, а записи в учёте нет.

– Дублирование записей: одну и ту же операцию провели дважды.

– Ошибки в датах: документ датирован прошлым годом, хотя операция была в этом.

– Несоответствие сумм: в накладной одна сумма, в учёте — другая.

– Отсутствие подписей или печатей: документ оформлен не полностью, его нельзя считать действительным.

Оформление результатов проверки

По итогам проверки составляют документ (акт или справку), где указывают:

– что проверяли (период, объекты);

– какие методы использовали (сверка, инвентаризация и т. д.);

– что обнаружили (нарушения, расхождения);

– рекомендации по исправлению (например, «внести в учёт пропущенные документы», «провести повторную сверку с контрагентом»).