

# Вопросы обеспечения безопасности деятельности региональных и муниципальных органов внешнего финансового контроля в условиях цифровой трансформации

Доклад председателя Счетной палаты Красноярского края Д.В. Воропаева  
на VII ежегодной научно-практической конференции  
«Угрозы и риски финансовой безопасности в контексте цифровой трансформации», СФУ  
25 ноября 2021 года

Добрый день, уважаемые коллеги!

Мое короткое выступление посвящено теме обеспечения безопасности деятельности региональных и муниципальных органов внешнего финансового контроля в условиях цифровой трансформации.

Хочу рассмотреть три основных аспекта. Это защита входящих информационных потоков, обеспечение информационной безопасности собственных информационных систем и баз данных, а также информации, выходящей за внешний контур.

Принятые в текущем году поправки в Федеральный закон от 07.02.2011 № 6-ФЗ «Об общих принципах организации и деятельности контрольно-счетных органов субъектов Российской Федерации и муниципальных образований» внесли существенные изменения в отношении статуса и правового регулирования деятельности контрольно-счетных органов. Указанные поправки вступили в силу 30.09.2021.

Важным обстоятельством в контексте сегодняшнего разговора явилось то, что, помимо прочих изменений, существенно обновились положения **статьи 15** нашего базового закона, которой регламентировано **представление информации контрольно-счетным органам**.

Так, в настоящее время при осуществлении внешнего государственного и муниципального финансового контроля контрольно-счетным органам предоставляется необходимый для реализации их полномочий постоянный доступ к государственным и муниципальным информационным системам в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, законодательством Российской Федерации о государственной и иной охраняемой законом тайне.

То есть, если ранее такой доступ мог быть предоставлен в рамках определенных договоренностей и заключенных соглашений (и, между нами говоря, не всегда был исчерпывающим), то отныне это императивная норма. Безусловно, это значительный и значимый шаг к повышению эффективности взаимодействия и контроля. Однако это также ставит нас перед новыми условиями защиты информации, доступ к которой нам предоставлен. И это достаточно серьезная проблема. Конечно, решаемая, но требующая привлечения дополнительных ресурсов.

Как вы знаете, система контрольно-счетных органов Российской Федерации, начиная от КСО поселений и заканчивая федеральной Счетной палатой, не является вертикально интегрированной. Собственно, это один из факторов, обуславливающих независимость внешнего финансового контроля.

Но такая независимость также может стать залогом того, что каждый отдельный контрольно-счетный орган вынужден в равной степени самостоятельно решать вопросы обеспечения своей деятельности (в том числе ее безопасности), не имея возможности использовать наработки коллег, поскольку это другой бюджет.

Следующие два аспекта, а именно обеспечение информационной безопасности собственных информационных систем и баз данных, а также информации, выходящей за внешний контур, тесно связаны с изменением подходов к осуществлению контрольной деятельности, обусловленных появлением новых возможностей, возникающих в ходе цифровой трансформации.

Речь идет о так называемом «цифровом инспекторе».

Это направление трансформации есть в плане мероприятий по цифровому госуправлению, а также интегрировано в соответствующий нацпроект.

Так, еще в апреле 2018 года правительство утвердило **Положение о ГИС «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»**, которое было актуализировано в текущем году.

И ряд федеральных ведомств уже включился в новый формат работы (Росприроднадзор, Росрыболовство, Федеральная таможенная служба, Федеральная налоговая служба, МЧС, Роструд).

Но, как вы понимаете, это опять не про нас, поскольку контрольно-счетные органы не входят в систему органов исполнительной власти и, следовательно, вынуждены идти своим путем.

Локомотивом в этом движении естественно выступает Счетная палата Российской Федерации.

Так, в составе ГИС «Информационно-телекоммуникационная система «Контроль» также осуществляется разработка **Комплекса программных средств «Цифровой инспектор»**, направленная на решение следующих задач. Это:

- Повышение эффективности планирования, организации и выполнения задач по осуществлению контроля за целевым и эффективным использованием бюджетных средств, бюджетов государственных внебюджетных фондов, аудита реализуемости и результативности достижения стратегических целей социально-экономического развития Российской Федерации;
- Сокращение трудоемкости основной деятельности КСО и повышение ее качества;
- Содействие повышению качества системы государственного управления;
- Повышение качества и увеличение объема государственных и иных данных, используемых при осуществлении внешнего аудита;
- Повышение объективности результатов проверок и анализа за счет применения современных аналитических инструментов, реализующих риск-ориентированный подход и предиктивную аналитику.

То есть «Цифровой инспектор» – это программно-аппаратный комплекс, предоставляющий пользователю возможность работы в режиме «единого окна» с консолидированной и обработанной оцифрованной информацией по объектам проверки, аккумулированной в едином хранилище данных, с применением современных аналитических инструментов, реализующих риск-ориентированный подход и предиктивную аналитику.

В рамках реализации проекта предусматривается:

- Внедрение аналитической платформы на базе новых технологий обработки и анализа данных, а также реализация широкого спектра аналитических функций;

- Широкий спектр функций различных модулей и систем, интегрированных между собой и объединенных в едином цифровом пространстве с целью обеспечения работы пользователя в режиме «единого окна»;

- Сбор, обработка, обеспечение качества и хранение данных из ряда внутренних информационных систем и большого перечня внешних источников в едином хранилище данных.

Как мы понимаем, в этом наше будущее.

В то же время принципиально новый подход к осуществлению контроля и анализа требует принятия надлежащих мер по защите используемой информации, особенно при проведении мероприятий на объектах, поскольку искажение данных или утечка информации могут иметь весьма и весьма существенные последствия, причем как для проверяемых, так и для проверяющих.

И здесь, как нам кажется, тоже необходим системный подход, требующий принятия решений на федеральном уровне, поскольку предельно ясно, что подавляющее большинство КСО самостоятельно не справятся с такой задачей. Речь здесь, конечно идет в первую очередь о муниципальном контроле, как наименее подготовленном к цифровой трансформации звене.

У меня все, спасибо за внимание!