# ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

# ДОСТОВЕРНОСТЬ ПРОИЗВОДСТВЕННЫХ УЧЕТНЫХ ДАННЫХ

Улиткин А.В., директор ООО «Октализ»

Основной целью создания коммерческого предприятия является получение прибыли. Опуская тонкости, прибылью можно назвать разницу между доходами от реализации продукции и расходами на её производство. Собственник заинтересован в получении максимальной прибыли, то есть наибольшей выручки от продаж при одновременной минимизации расходов на производство.

Расходы включают в себя не только прямые затраты на производство, включая отходы и брак, но и хищения. Предотвращениями хищений или каких-либо мошеннических действий с товарно-материальными ценностями (ТМЦ) занимаются особые службы, отвечающие за безопасность компании. Эффективность их работы напрямую влияет на экономические показатели деятельности предприятия, поскольку существенно уменьшают издержки производства.

Стандартный алгоритм выявления мошеннических действий с ТМЦ включает проведение регулярных аудиторских проверок. В основном речь идет о проведении ревизий на складах и производственных участках. Безусловно, подобные физические мероприятия весьма эффективны, поскольку позволяют не только выявлять хищения, но и являются серьезной мерой профилактического характера.

Серьезные производственные компании, стремящиеся максимально эффективно управлять технологическими процессами, оснащают производственные участки и склады автоматизированными системами управления процессами хранения и движения ТМЦ. Проведение ревизии при наличии такой автоматизированной системы заключается в банальной распечатке отчёта и сверке с фактически находящимися на складе (производственном участке) ТМЦ.

Этот метод является самым эффективным в плане выявления фактов отклонения данных о физических запасах ТМЦ от данных, хранящихся в учетных системах компании.

Однако у него есть существенный недостаток: ревизия, позволяющая выявить расхождения фактических запасов и данных в ИС, но не всегда позволяет обнаружить факты хищения ТМЦ.

Дело в том, что вся информация о ТМЦ хранится в информационных системах, которые порой являются единственным источником формирования учетных и бухгалтерских документов на производственной площадке. Именно этим зачастую этим пользуются мошенники в своих корыстных целях. Речь идет не о хакерах, взломавших информационную систему (хотя такое тоже вполне возможно), а о сотрудниках предприятия, действия которых направлены на искажение производственных учетных данных.

**Тем или иным способом оказывая воздействие на процессы производственного учета, в том числе автоматизированные, мошенники**

**достигают нужного им результата: информация о ТМЦ оказывается представленной не «как есть», а как нужно им. Преднамеренно внося искажения в производственные учетные данные или организуя их формирование особым образом, мошенники создают основу для хищения или скрывают факты нанесения материального ущерба компании.**

Проведение ревизии в классическом виде становится бессмысленным, поскольку мошенники позаботились о соответствии данных в ИС и наличествующих ТМЦ. Аудиторы получат идеальный результат полного соответствия либо минимальные отклонения, которые будут объяснены человеческим фактором, погрешностью контрольно-измерительных приборов, сбоем оборудования и т.п.

Как показала практика, угроза хищения или мошеннических действий с использованием различных методов искажения учетных данных присутствует на большинстве промышленных предприятий. Высокий уровень автоматизации технологических и производственных процессов нередко не только не помогает выявлять хищения, но, напротив, помогает мошенникам.

Пользуясь высоким доверием людей к информационным технологиям, мошенники легко представляют искаженные учетные данные в качестве абсолютной, непоколебимой истины.

## ТОЧКИ РИСКА ИСКАЖЕНИЯ ПРОИЗВОДСТВЕННЫХ УЧЕТНЫХ ДАННЫХ

Для того чтобы более детально разобраться с проблемой злонамеренного искажения учетных данных, следует понять, какая именно информация критична и каким образом она может быть искажена.

Говоря о производственных учетных данных, нужно понимать, что для каждого предприятия и даже для каждого цеха набор критичных данных будет разнится. Но критичные для производственного учета данные можно представить тремя общими для всех группами:

- информация, идентифицирующая ТМЦ (в частности, сырье, полуфабрикаты и готовую продукцию);
- информация о процессах производства, хранения и перемещения вышеуказанные ТМЦ;
- информация о качественных параметрах (характеристиках) ТМЦ.

Системы управления промышленным предприятием представляют собой вертикально интегрированную структуру из трех уровней, на каждом из которых работают разные типы информационных систем:

- автоматизированные системы управления технологическим процессом (АСУ ТП);
- автоматизированные системы управления производством (АСУ П);
- автоматизированные системы управления предприятием.

Разные виды вышеперечисленных данных о ТМЦ формируются, хранятся и передаются между всеми уровнями комплекса корпоративной информационной системы.

Количество основных операций с данными в рамках одной вертикали АСУ ТП – АСУ П – АСУ составляет больше десятка. И многие из этих операций представляют собой **точки риска искажения производственных учетных данных**, которыми могут воспользоваться злоумышленники.

## ПОЧЕМУ КЛАССИЧЕСКИЕ СРЕДСТВА ИБ БЕССИЛЬНЫ?

Возникает вопрос об использовании средств защиты информации как достаточного решения, обеспечивающегося достоверность производственных учетных данных. Даже у руководителей подразделений по безопасности создается впечатление, что достаточно грамотно создать защиту критичных для учета ТМЦ данных в информационных системах, и проблема будет решена. К сожалению, это не так.

Правильно будет заметить, что для защиты информации, обеспечения её целостности и достоверности существует большое количество решений в области информационной безопасности. Они действительно позволяют и контролировать действия пользователей, и выявлять подозрительные либо нестандартные действия в ИС. Современные системы защиты информации контролируют даже святая святых ИТ-специалистов – действия администраторов, делая прозрачными все процессы внесения изменений в систему.

Многие крупные производственные компании используют, по их собственным утверждениям, системы типа DLP для обеспечения достоверности производственных учетных данных и считают, что этого достаточно. DLP-системы направлены на предотвращение утечки данных, и теоретически их функционал по выявлению подозрительных действий сотрудников в ИС может использоваться для обеспечения достоверности учетных данных. Но только в случае, если злоумышленники напрямую корректируют информацию о ТМЦ в разрез с утвержденными бизнес-процессами и их действия являются «подозрительными».

Но что такое «подозрительные действия» в информационной системе? Ведь если пользователь выполняет какие-то действия в программе, работающей с критичными для производственного учета данными, то он пользуется тем инструментарием, который ему предоставлен официально, то есть использует полномочия, согласованные в рамках процессов управления доступом. Получается, что в пределах легитимных бизнес-процессов, используя утвержденный в компании функционал программного обеспечения, сотрудник имеет возможность выполнять неправомерные или подозрительные операции. Возникает вопрос, а зачем тогда ему предоставлен такой функционал?

Говоря о системах защиты информации применительно к вопросу достоверности производственных учетных данных, необходимо понимать принципы их формирования и последующей работы с ними. Большинство систем защиты информации были первоначально разработаны и использовались в банковской сфере. Именно банковский бизнес в какой-то мере считается пионером в области внедрения технологий защиты информации.

В дальнейшем, положительно зарекомендовав в себя, аналогичные решения стали использоваться в ИС промышленных компаний. Широкое применение они

получили в системах уровня управления предприятием. Однако использования только систем по защите информации и различных аналитических (аудиторских) систем в случае с производственными учетными данными явно недостаточно. Они не могут полностью устранить угрозы и минимизировать риски искажения производственных учетных данных. Все дело в сути защищаемых «объектов», принципах работы систем, а также в среде, где выполняются операции над охраняемыми ценностями.

Если рассматривать защиту данных в банковском секторе, то защищаемым объектом является сам «товар», то есть деньги, данные о которых хранятся в ИС. Основной «производственный процесс» работы с деньгами выполняется непосредственно в информационных системах. Именно ИС являются главным инструментарием работы с товаром – деньгами, поэтому информационные системы безопасности способны контролировать весь «технологический процесс».

На производственном предприятии всё иначе. Производственный процесс представляет собой ряд технологических операций, выполняемых по отношению к реальным физическим объектам: сырью, полуфабрикатам и готовой продукции. В информационных системах хранятся лишь данные о ТМЦ, которые носят описательный характер. В ИС заносятся результаты производства и операции с ТМЦ. Сами операции производства, перемещения и хранения выполняются вне виртуальной среды информационных систем, поэтому классические системы защиты информации контролируют «проекцию» операций над ТМЦ.

**Нужно понимать, что вопросы достоверной системы учета промышленного предприятия выходят за рамки одних лишь информационных систем. Именно поэтому они многократно превышают зону ответственности ИТ-подразделения.**

ИТ-подразделение – это сервисная структура, выполняющая заказ других подразделений компании на автоматизацию бизнес-процессов и технологических функций. Программные продукты и решения создаются на основании сформированных потребностей и требований основных и вспомогательных бизнес-подразделений. Последние формируют и утверждают функциональные и технические задания, определяют функциональные принципы обработки и представления информации, реализуемые в дальнейшем в программном обеспечении.

Автоматизированные функции работы с учетными данными – это часть комплексной учетной системы компании. Риски формирования неточной или искаженной информации в комплексной корпоративной учетной системе могут проецироваться на автоматизированные процессы и привести к искажению критичных данных.

Комплексная учетная система компании не нечто самодостаточное. Это объединение управленческих направлений, формирующих производственный учет и влияющих на него. По идее, все технологические и сервисные операции должны основываться на определенных регламентных документах и инструкциях. Комплекс корпоративных технологических, нормативных и регламентных документов является основой для корпоративной учетной системы. Отсутствие полноценного базиса в виде вышеописанных документов, пробелы или

неисполнение регламента приводит к угрозам формирования недостоверных учетных данных.

Зачастую эти проблемы по отношению к комплексной корпоративной учетной системе возникают в результате следующих нарушений:

- ✓ несовершенство технологических документов;
- ✓ несовершенство нормативно-регламентной базы;
- ✓ несовершенство функционала информационных систем;
- ✓ отсутствие комплекса эффективных контрольных процедур.

В формировании комплексной корпоративной учетной системы участвуют практически все основные подразделения компании. Эта проблема не может быть решена силами одного подразделения. Логически подразделения можно разделить на три группы: создающие основу для учетной системы, реализующие автоматизированные функции учета, составляющие требования и контролирующие их выполнение.

Подразделения, отвечающие за формирование нормативной базы учетной политики, которые непосредственно создают и используют учетные данные:

- ✓ производственное подразделение и структура, отвечающая за управление производством;
- ✓ технологическое подразделение, отвечающее за подготовку производства;
- ✓ подразделение контроля качества;
- ✓ логистическое подразделение;
- ✓ прочие сервисные подразделения.

Бухгалтерия и управление экономики являются пользователями учетной данных и, в свою очередь, формируют требования к составу данных, поступающих к ним от других подразделений.

Подразделения, участвующие в формировании требований к учетным данным, описывающие риски и в дальнейшем контролирующие их выполнение, относятся к группе обеспечивающих безопасность компании:

- ✓ подразделение экономической безопасности;
- ✓ служба безопасности, включая информационную безопасность;
- ✓ контрольно-ревизионное подразделение.

ИТ-подразделение выполняет автоматизацию процессов учета на основе подготовленной нормативной базы и контрольных процедур.

Уже на основании существующей качественной учетной политики возможна разработка контрольных процедур и внедрение организационно-технических решений (в том числе в сфере информационной безопасности), направленных на обеспечение достоверности учетных данных.

Создание полноценной корпоративной учетной системы – задача далеко не простая. Учитывая, что ответственность за сохранность собственности лежит на подразделении, отвечающем за вопросы безопасности, именно ему при решении проблем достоверности учетных данных приходится выступать в качестве организатора процессов построения системы учета.

Как правило, еще на стадии подготовки этих процессов возможно проявление проблем организационного характера. Возможно, что некоторые подразделения сформировали неполный перечень процедур учета ТМЦ в рамках своих производственных и бизнес-процессов. Это объясняется отсутствием четких требований в области учета, который вызван эффектом «пограничных» бизнес-процессов и рабочих функций подразделений. Или, отстраняясь от пограничных процессов, подразделения перекладывают выполнение отдельных функций друг на друга. В итоге многие вопросы, связанные с производственным учетом и, в частности, с обеспечением его достоверности, повисают в воздухе.

В частности, речь идет о реализации функции ручной корректировки данных о результатах производства. Потребность в данной функции формирует структура управления производством. Все остальные службы используют результаты программного функционала, но их не интересует корректность его использования:

1. разработчики программного обеспечения реализуют функцию ручной корректировки;
2. служба информационной безопасности «пропускает» ее, поскольку это стандартный функционал, который не может считаться нарушением;
3. для бухгалтерии данные вопросы и вовсе не интересны: подразделение оперирует теми данными, которые взяты из системы;
4. служба безопасности тоже не касается данного вопроса, поскольку он не связан с физическим хищением ТМЦ.

Помимо  простого нежелания выполнять «чужую» работу аналогичные ситуации могут быть вызваны некомпетентностью работников. Приняв к исполнению сложные функции, они оказываются не в состоянии их выполнить.

Стоит отметить еще один важный момент. Поскольку мошенничеством занимаются люди, работающие в компании, то проблемы с системой производственного учета могут быть созданы преднамеренно, то есть искусственно. Формирование «управляемого хаоса» на руку мошенникам, которые знают реальную картину происходящего и используют ее в своих корыстных целях.

Прежде чем начинать разбираться в проблемах производственного учета, стоит по-новому взглянуть на результаты проводимых на промышленных площадках и складах ревизий.

Можно задаться вопросом: а есть ли смысл в проведении ревизии, если существует риск (угроза) искажения учетных данных и реальной картины? Может быть, не стоит тратить время и ресурсы на аудиторские проверки, пока на 100% мы не будем уверены в достоверности данных? Безусловно, проводить ревизии необходимо. Только интерпретировать результаты необходимо с учетом возможных рисков недостоверности учетных данных.

Поскольку речь идет о комплексной корпоративной системе учета, то анализировать результаты ревизий нужно не по одному участку, а по нескольким. Чем больше результатов ревизий будет получено по разным производственнымучасткам в короткий промежуток времени, тем лучше.

Возможно три варианта результатов проведенной ревизии.

1. Выявлена недостача ТМЦ. Они либо похищены, либо произошел сбой в системе учета ТМЦ. (Не обязательно в информационной системе: может иметь место человеческий фактор). В данном случае говорить о достоверности учетной системы нет смысла. Возможно, аудиторы провели проверку до момента внесения изменений в ИС и приведения её в соответствие с фактическим количеством ТМЦ.
2. Соответствие ТМЦ и данных из информационной системы. Результат ревизии в привычном понимании подтверждает отсутствие фактов хищения и внешне свидетельствует о том, что система учета работает нормально. С другой стороны, за внешним благополучием может быть скрыта мошенническая схема, то есть ревизоры увидели результаты работы мошенников.
3. Избыточное неучтённое ТМЦ. Данный результат может вызвать неоправданное радостное удивление. Оказывается, что запасов больше, чем предполагалось. Однако именно этот результат самый печальный. Он говорит о стопроцентном сбое в системе учета ТМЦ, причем как вследствие человеческого фактора, так и в результате обнаружения мошеннической схемы. К примеру, «лишние» ТМЦ приготовили к вывозу.

Обеспечение достоверности производственных учетных данных не является самоцелью. Это решение должно обеспечивать противодействие скрытию фактов мошенничества с целью обогащения за счет компании. На основании достоверной системы учета в комплексе с эффективной системой управления производством возможно выявление недостачи и хищений ТМЦ в автоматическом режиме.

Алгоритм мошеннических действий с учетными данными ТМЦ на производственном предприятии заключается в последовательном выполнении двух базовых действий:

1. искажение данных о стоимости ТМЦ или удаление данных о ТМЦ из учетной системы;
2. монетизация сокрытой стоимости.

Сами по себе товарно-материальные ценности не представляют для мошенников интереса. Ценностью являются деньги, которые можно получить после их реализации. Каким образом работает алгоритм? Об этом читайте в следующей статье.