Внимание!!! Данная статья ранее была опубликована в научном журнале. При использовании материалов для написания научных трудов просьба оформлять ссылку на первоисточник

Ссылка для списка литературы:

Татаров К.Ю. Учет затрат на содержание объектов критической информационной инфраструктуры // Бухгалтерский учет. 2020. № 4. С. 95-100

Учет затрат на содержание объектов критической информационной инфраструктуры

К.Ю. Татаров,
кандидат экономических наук,
Главный бухгалтер
ООО «Группа компаний «ДЕКАРТ»,
г. Москва.
E-mail: ktatarov@mail.ru

Внедрение в повседневную жизнь компьютерных технологий, развитие телекоммуникационного сообщения и прочие информационные технологии стали предпосылками нового вида преступной деятельности – кибератак с использованием всемирной сети Интернет. Мировые убытки от подобных преступлений стали исчисляться миллионами долларов. В целях государственной защиты информационного пространства принят Федеральный закон от 26 июля 2017 года N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Данный законодательный акт вводит в практику новый термин "критическая информационная инфраструктура (КИИ)", определяя ее как информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

К субъектам КИИ закон относит Государственные органы, государственные учреждения, российские юридические лица и (или)

индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат объекты КИИ. В тексте закона определено тринадцать направлений деятельности, на которые распространяются данные нормы, в частности это области науки, транспорта, связи, энергетики, банковской сфере и многих других. Данный перечень является закрытым, следовательно на иные виды деятельности рассматриваемые нормы не распространяются.

Данный закон рассматривает КИИ, эксплуатируемую каким-либо субъектом, как элемент общей системы информационной безопасности, регламентируемой на государственном уровне и рассматриваемой уже с точки зрения государственной безопасности. Для учета, анализа и принятия своевременных мер по противодействию компьютерному и информационному терроризму формируется государственная система идентификации и устранения последствий компьютерных атак на информационные системы Российской Федерации – ГосСОПКА.

Данный закон не подразделяет субъектов ККИ на собственников или не собственников. Следовательно, учет затрат на содержание и эксплуатацию объектов КИИ должен быть организовываться вне зависимости от способа отражения подобных объектов в регистрах бухгалтерского учета, а также наличия или отсутствия права собственности.

Учет затрат на категорирование объектов КИИ

Количество объектов IT-инфраструктуры, принадлежащих юридическим лицам, и используемых в указанных в законе видах деятельности, не поддается исчислению. Поэтому, Федеральный закон вводит понятие "категорирование". Под данным термином понимается процедура оценки объектов КИИ с точки зрения влияния на безопасность жизнедеятельности общества. Например, компьютерный вирус, уничтоживший информацию на компьютере менеджера по продажам в коммерческой фирме, вызовет только досаду пользователя и затраты на

восстановление поврежденной оргтехники. Если тот же самый вирус проникнет в систему управления воздушным движением и вызовет ее сбой, то под угрозой безопасность окажется работоспособность целого сегмента экономики, а ровно и множество человеческих жизней.

Процедура категорирования определена в Постановлении Правительства от 8 февраля 2018 г. (ред. от 13.04.2019) №127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений". В данном постановлении определены четырнадцать видов негативных последствий, к которым может привести сбой в работе объектов КИИ.

В соответствии с пунктом 11 данного Постановления, для проведения категорирования в организации создается постоянно действующая комиссия по категорированию, в состав которой включаются:

а) руководитель субъекта или уполномоченное им лицо;

б) работники, являющиеся специалистами в области осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

в) работники, на которых возложены функции обеспечения безопасности (информационной безопасности);

г) работники подразделения по защите государственной тайны;

д) работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций.

Данная комиссия создается приказом руководителя организации и действует на безвозмездной основе. Точки зрения бухгалтерского учета, члены комиссии выполняют свои обязанности на общественных началах без начисления заработной платы. Данная комиссия продолжает осуществлять

свою деятельность также и после окончания процедуры категорирования, так как информационные сети и объекты КИИ в течении хозяйственной деятельности будут реконструироваться, модернизироваться, расширяться, ремонтироваться и т.д. Все подобные технические перевооружения будут влечь за собой очередной этап работы комиссии. Таким образом, членство в данной комиссии сопряжено с большим объемом временных и трудовых затрат.

С точки зрения трудового права и бухгалтерского учета, работа подобной комиссии может быть оформлена как:

Расширение уже действующего функционала работников. Принимая во внимание, что членство в комиссии будет отнимать у работников много времени, имеет смысл пересмотреть должностные инструкции некоторых работников.

Оформление отношений с работниками посредством подписания Договора возмездного оказания услуг, как на период категорирования, так и в будущем при техническом перевооружении. Подобный подход позволит материально заинтересовать работников и создать им возможность осуществление функций члена комиссии с минимальным ущербом основной работе. В частности, у сотрудника будет иметься стимул для работы в выходные дни, в вечернее время или использование аналогичных временных резервов.

Вместе с тем, данный вопрос, по нашему мнению, может быть решен сторонней организации на основании хозяйственного договора. Подобный подход на практике будет иметь ряд преимуществ:

✓ Привлечение к работе специалистов, которые являются профессионалами в своей области. Сотрудники организации не всегда могут оказаться компетентными в вопросах информационной безопасности и не всегда правильно могут смоделировать потенциальную опасность. Как следствие, категорирование объектов КИИ может оказаться некорректным

✓ Исключение споров и разногласий. В случае некачественного выполнения работ, споры решаются на уровне хозяйствующих субъектов. При этом исключается возможность перевода конфликта в трудовые отношения, риск которого присутствует во внутренней комиссии;

✓ Отсутствие проблем с государственными службами. Все необходимые документы, созданные в период категорирования, грамотно оформляются и своевременно представляются в государственные структуры (ГосСОПКА, центральный аппарат Федеральной службы по техническому и экспортному контролю (ФСТЭК) и другие). Исполнение этого требования внутренней комиссией может оказаться проблематичным;

✓ Повышение эффективности работы собственного персонала и избавление его от выполнения непрофильных функций. Это дает возможность высвободившимся работникам сконцентрироваться на основной трудовой функции;

✓ Получение от организации – подрядчика профессиональных консультаций и рекомендаций по функционированию, эксплуатации и защите объектов КИИ после окончания процедуры категорирования.

В регистрах бухгалтерского учета отражение затрат на оплату услуг сторонней организации, выполняющей услуги по категорированию объектов КИИ, следует рассматривать как общехозяйственные расходы, так как подобные объекты являются общими для всех структурных подразделений организации и выделить из них отдельные составляющие не представляется возможным.

Производятся следующие записи в бухгалтерских регистрах:

Д-т сч. 26 "Общехозяйственные расходы";

К-т сч. 76 "Расчеты с разными дебиторами и кредиторами"

Дальнейшее закрытие счета 26 "Общехозяйственные расходы"; осуществляется в соответствии с учетной политикой организации.

Что касается налогового учета, то подобные затраты следует признать экономически обоснованными, так как они направлены на выполнение

требований федерального законодательства. Полученные от подрядной организации первичные документы, в свою очередь, послужат документальным подтверждением произведенных расходов. Эти два элемента позволят признать затраты на категорирование объектов КИИ, выполненное сторонней организацией, расходами для целей применения главы 25 НК РФ.

В результате работы специализированной компании может получиться так, что у заказчика вообще не будет выявлено объектов КИИ, подлежащих категорированию. В этом случае, подобные объекты будут обозначены, как «без категории». Подобный результат не является основанием для признания произведенных расходов экономически необоснованными. Более того, если подобный результат определен независимой компанией, организации-заказчику легче будет обосновать подобный "безкатегорийный" вывод в случае отраслевой проверки, так как в период работы отсутствовало возможное давление на членов комиссии со стороны руководства организации и тем самым была обеспечена большая непредвзятость полученных выводов. Если же подобный результат будет получен внутренней комиссией, у проверяющих может сложиться впечатление специального признания объектов "безкатегорийными" в целях минимизации текущих расходов и уменьшения документооборота с государственными органами.

Учет последствий кибератаки

Информационные угрозы достигли таких размеров, что Советом Европы была принята Европейская конвенция по борьбе с киберпреступностью. Этот международный пакт выделил следующие типы преступлений, совершаемые при помощи компьютерных технологий.

- незаконное проникновение,
- электронное мошенничество
- кража интеллектуальной собственности.

Незаконное проникновение представляет собой подключение (взлом) объектов КИИ с различными противозаконными целями. Это может быть кража базы данных, получение конфиденциальной информации, или просто вывод системы из строя без определенной цели. Как правило, подобный вид кибератаки возможен только против некрупных компаний, не имеющих возможности содержать собственное подразделение информационной безопасности, и работающими по открытым канала телекоммуникационной связи. С точки зрения бухгалтерского учета подобное злодеяние не несет прямых затрат. Однако, в этом варианте присутствуют материальные затраты на восстановление работоспособности системы. Подобные затраты могут оказаться вполне существенными, так как может понадобиться помощь сторонних специалистов. Расходы на подобное исправление ситуации, по нашему мнению, стоит отображать через счет 91 "Прочие доходы и расходы", как не имеющие отношение к формированию себестоимости выпускаемой продукции и не относящимся к общехозяйственным расходам.

Д-т сч. 76 "Расчеты с разными дебиторами и кредиторами"

К-т сч. 51 "Расчетные счета";

Д-т сч. 91 "Прочие доходы и расходы";

К-т сч. 76 "Расчеты с разными дебиторами и кредиторами"

Подобные расходы найдут свое отражение по дебету субсчета 2 "Прочие расходы", что соответствует Инструкции по применению плана счетов финансово-хозяйственной деятельности организации.

С точки зрения налогового учета подобные расходы следует квалифицировать как внереализационные и признать расходами для целей налогообложения, согласно подпункту 20 пункта 1 статьи 265 НК РФ. У налогоплательщиков к внереализационным расходам относятся любые расходы, не связанные с производством и (или) реализацией, и не относящиеся к расходам, не учитываемым в целях налогообложения.

Электронное мошенничество представляет собой хищение чужого имущества или приобретение права на чужое имущество путем обмана с использованием компьютерных технологий.

С точки зрения бухгалтерского учета подобный вид преступления может проявляться в хищении денежных средств организации. Как любое уголовное преступление электронное мошенничество является объектом расследования правоохранительных органов. Однако, для приведения регистров бухгалтерского учета в соответствие с текущим положением дел, украденные суммы следует списать с расчетного счета в корреспонденции с отдельным субсчетом, открываемом к счету 76 "Расчеты с разными дебиторами и кредиторами". На данном субсчете, рассматриваемые суммы должны числиться до момента завершения расследования и получения официального документа, что найти киберпреступника не представляется возможным.

Министерство финансов в своем письме от 17 декабря 2018 года № 03-03-06/1/92021, ссылаясь на статью 265 Налогового кодекса, указало, что учитывать убытки от хищения денежных средств со счетов для целей налога на прибыль можно в составе внереализационных расходов. Таким образом, по окончанию следственных мероприятий, учтенные суммы признаем расходом как в бухгалтерском учете (на дебете счета 91 "Прочие доходы и расходы"), так и в налоговых регистрах.

Кража интеллектуальной собственности являет собой нарушение авторских прав, то есть противоправное использование научных достижений, а также тиражирование произведений культуры. В этом случае, результат кибератаки носит отложенный во времени характер. Законный правообладатель получает убыток не единовременно в момент взлома системы, а спустя определенное время. По прошествии определенного периода начинается использование (тиражирование) объекта кражи, и законный правообладатель начинает фиксировать падение прибыли.

В отличие от двух ранее рассмотренных вариантов убытков от компьютерных преступлений, кража интеллектуальной собственности

напрямую затрагивает регистры бухгалтерского учета. Результаты интеллектуальной собственности, в соответствии с правилами бухгалтерского учета, подлежат отражению на балансовом счете 04 "Нематериальные активы". Кража и незаконное тиражирование, или иное использование подобного актива, резко снижает его текущую коммерческую стоимость. В сложившейся ситуации, по нашему мнению, организации может использовать один из двух инструментов. Списать данный нематериальный актив полностью или произвести пересмотр его стоимости (уценить). Выбор между этими двумя вариантами должна сделать комиссия, которая будет создана приказом руководителя. Если последствия компьютерной кражи актива носит объемный характер и подрывает монополию организации на его использование, имеет смысл говорить о полном списании данного нематериального актива, так как он перестает удовлетворять требованиям, обозначенным в ПБУ-14/2007 "Учет нематериальных активов". Если же актив, не смотря на его незаконное тиражирование, еще обладает способностью приносить экономические выгоды, хоть и не в прежних масштабах, объект подлежит уценке. В результате, на дебете счета 04 "Нематериальные активы" окажется текущая, рыночная стоимость объекта.

При использовании любого из двух вариантов, будет изменена первоначальная и остаточная стоимости похищенного актива. Следовательно, этот факт найдет свое отражение по соответствующей статье бухгалтерского баланса, и вызовет резкое изменение валюты баланса текущего года. Подобный факт должен быть раскрыт в пояснительной записке к годовой бухгалтерской отчетности. Необходимо помнить, что подобные изменения порождают отрицательный результат вертикального финансового анализа, проводимого заинтересованными пользователями. Также это негативно скажется на расчете коэффициентов ликвидности и определения финансовой устойчивости и инвестиционной привлекательности организации.

Отражение информации о кибератаках в управленческом учете

Такое явление как кибератака находит свое отражение не только в официальной и технической статистике, или в финансовом учете, но и в управленческом учете организации. Однако, расчет и признание расходов в данном случае рассчитывается по иному алгоритму. Данные подобного расчета не обнародуются, но могут играть огромную роль в процессе управления организацией.

Величины расходов в управленческом учете может быть определена на основании фактических величин, а также рассчитана математическими методами.

Фактическая величина может быть взята из данных финансовой отчетности. Подобным образом признается расход от обвала котируемых акций на бирже. В соответствии с российским корпоративным законодательством, компьютерная атака не признается существенным фактом и не подлежит раскрытию для заинтересованных пользователей (инвесторов, акционеров и пр.). Если факт атаки становится достоянием общественности и последствия являют собой величину, сопоставимую с активами организации, это может вызвать падение котировок объекта атаки. Сумма уменьшения капитализации эмитента будет признаваться расходов в управленческом учете.

Для определения величины расходов математическими методами необходимо учитывать как конъюнктуру рынка, там и место на нем организации, подвергшейся кибератаке. В частности, необходимо учитывать упущенную выгоду или падение репутации организации.

Упущенная выгода может быть рассчитана как величина недополученных доходов, уменьшенных на величину предполагаемых расходов. Основанием для расчета выступают данные бухгалтерской отчетности с учетом временного фактора. Если в результате кибератаки организации пришлось списать нематериальный актив, то расчет будет осуществляться от средней величины экономических выгод, возникающих в

результате прежней эксплуатации объекта, умноженной на срок предполагаемого использования.

Пример: На балансе организации имеется уникальная рецептура переработки свежей ягоды, обозначенная как know how, и учтенная в качестве нематериального актива. Рецептура использовалась в производстве, позволяла организации быть монополистом и получать максимальную прибыль. После несанкционированного взлома компьютерных баз, данная рецептура была обнародована в сети Интернет и стала достоянием всех заинтересованных пользователей, в том числе конкурентов. Организация обратилась в соответствующие органы с требованием блокировки сайтов, на которых была предана огласке подобная информация. Выявленные сайты были заблокированы, однако общее количество задействованных ресурсов определить не представляется возможным. Также не поддается учету и анализу количество сделанных копий данной информации. В результате кибератаки информация, ранее составляющая коммерческую тайну организации, была разглашена, и в обозримом будущем можно ожидать появления аналогичной продукции конкурентов. Монопольному положению организации на рынке был нанесен невосполнимый ущерб. В месяц продавалось продукции, изготовленной по данному рецепту, на сумму 300 тыс. руб. Организация рассчитывала использовать рецептуру в течении 10 лет. Рентабельность производства составляла 20 процентов.

Упущенная выручка: 300000 * 10 лет * 12 мес. = 36000000 руб.

Упущенная прибыль: 36000000*20%=7200000 руб.

Данные суммы в финансовом учете и бухгалтерской отчетности никогда отражены не будут, поэтому заинтересованные пользователи ознакомиться с ними не представляется возможным. Однако, с точки зрения управления компанией будут сделаны очень важные выводы. В частности, компании придется пересматривать бизнес-планы развития и бюджеты поступлений денежных средств,

так как рассматриваемые суммы ранее были учтены в процессе бюджетирования.