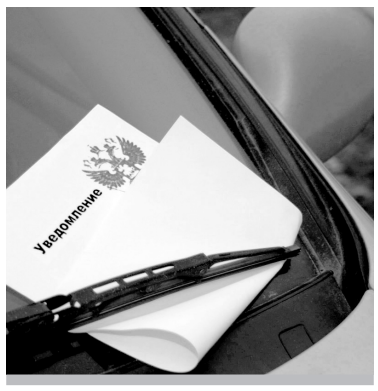
НАЛОГОВАЯ ИНСПЕКЦИЯ

МЕЖРАЙОННАЯ ИФНС РОССИИ № 9 ПО ПЕРМСКОМУ КРАЮ НАПОМИНАЕТ О СРОКЕ УПЛАТЫ ТРАНСПОРТНОГО НАЛОГА

В СООТВЕТСТВИИ С ЗАКОНОМ ПЕРМСКОГО КРАЯ ОТ 31.10.2011 № 855-ПК СРОК УПЛАТЫ ТРАНСПОРТНОГО НАЛОГА ЗА 2010 ГОД ПЕРЕНЕСЕН НА 15 НОЯБРЯ 2011 ГОДА



Хотелось бы обратиться к жителям района, что в случае если Вами не получено уведомление на уплату транспортного налога по текущим платежам, то необходимо подойти в Инспекцию по месту регистрации.

Оплату налога можно произвести разными способами, в том числе, через банкоматы и терминалы Западно-Уральского банка ОАО «Сбербанка России» можно оплатить задолженность по транспортному, земельному налогам и налогу на имущество физических лиц, набрав на терминале свой ИНН. Для осуществления платежа необходимо в меню «Штрафы и налоги» выбрать пункт «Задолженности по налогам (по ИНН)» и ввести 12-значный ИНН плательщика. Система проверит введенный ИНН на корректность и выведет на экран список имеющейся задолженности владельца. Услуга распространена по всей территории Пермского края, с возможностью оплаты как с банковской карты, так и наличными денежными средствами, без комиссии.

Режим работы Инспекции можно узнать на сайте Управления www.r59.nalog.ru. или по телефонам CALL-центра 211-47-17 или 8-800-100-5901 (звонок на всей территории края бесплатный).

Специалистами call-центра представляется информация об Индексе платежного документа (уникальный номер из 15 цифр) с помощью которого можно своевременно уплатить транспортный налог через банкоматы и платежные терминалы Сбербанка в разделе информационного поля «Платежи в нашем регионе»/ «Штрафы, налоги, госпошлины»/ «Текущие налоги (по индексу документа)»/ «Налоговые платежи текущие». Единственная просьба, при обращении к специалистам call-центра, быть готовым назвать свой ИНН, иметь при себе ручку и бумагу, чтобы записать цифры индекса платежного документа.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОФИСЕ

Целью информационной безопасности является предотвращение потери важной информации, а также противоборство несанкционированному доступу к конфиденциальной информации.

Информационная безопасность в любой организации достигается комплексом методов и средств защиты, а также организационными мероприятиями.

В большинстве случаев, когда заходит разговор о защите информации, в первую очередь начинают рассматривать программные или аппаратные средства, предотвращающие несанкционированный доступ к информации или защищающие от вирусов. Они безусловно необходимы, но любая защита бессильна перед человеческим фактором.

К сожалению, все ещё распространенной является картина отсутствия паролей на вход в компьютер, либо бумажки с паролями находятся прямо на рабочих местах. При выходе пользователей из кабинета компьютеры не блокируются, диски с данными и флешки хранятся в не достаточно защищенных от доступа посторонних лиц местах. Кроме того, не организовано разграничение прав доступа к данным, и любой сотрудник или злоумышленник может скопировать конфиденциальную информацию.

Для уменьшения рисков, связанных с информационной безопасностью, следует регламентировать список разрешенных для использования на рабочих местах программ. Зачастую, самостоятельно устанавливаемые пользователем приложения, скачанные из интернета, могут маскироваться под полезные и содержать в себе вредоносные программы или нарушить компьютерную безопасность.

В зависимости от информационной структуры организации необходимо подобрать соответствующие средства защиты: персональные антивирусы, сетевые экраны, защита шлюзов, файловых серверов и т.д. - исключить все возможные пути возникновения угроз. Особенно важна правильная настройка сетевой инфраструктуры, операционных систем и приложений для обеспечения должного уровня безопасности.

Основным средством защиты информации является резервное копирование данных. Его следует проводить регулярно, желательно в автоматическом режиме. Хранить копии можно на внешних носителях, защищенных от сбоев серверах или на специальных накопителях. Отдельно в защищенном месте следует хранить регистрационные данные и пароли.

Также важными организационно - техническими методами обеспечения информационной безопасности являются: разграничение прав доступа к информации и настройкам, регулярная смена паролей, использование лицензионного программного обеспечения, обучение пользователей безопасной работе с информацией, ограничение использования дисков и флеш-накопителей.

Если организация обрабатывает или хранит персональные данные физических лиц, то в соответствии с Федеральным законом РФ № 152 «О персональных данных» должны быть соблюдены обязательные требования по защите информационных систем персональных данных (ИСПДн). Для этого, приказом руководителя организации необходимо сформировать комиссию и присвоить своей ИСПДн соответствующий класс, разработать Положение по обеспечению безопасности персональных данных, утвердить список лиц, допущенных к обработке персональных данных (ПДн), а также некоторые другие документы. При необходимости в письменной форме получить согласие субъектов персональных данных на обработку своих ПДн. В соответствии со статьей 22 ФЗ-152 организация обязана уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) о своем намерении осуществлять обработку ПДн.

Как видим, государство серьезно вмешалось в процесс обеспечения безопасности персональных данных. Стоит отметить, что мероприятия по защите информации довольно трудоемки и могут привести к значительным финансовым затратам (привлечение лицензированных специалистов по созданию системы защиты ИСПДн, установка сертифицированных средств защиты информации), но все эти меры безусловно нужны и важны в современном обществе, в котором персональная информация обладает большой ценностью.

Компания «ВИРТУС Групп» занимается внедрением информационных систем на базе системы «1С». В своей работе мы используем описанные выше принципы соблюдения информационной безопасности и рекомендуем придерживаться их всем нашим клиентам.

Технический Директор
ООО «ВИРТУС Групп»
НИКОНОРОВ К. С.

www.virtusgroup.ru
sales@virtusgroup.ru

МИНИМАЛЬНЫЙ УРОВЕНЬ ЗАЩИТЫ

1. Установить пароли на доступ к компьютерам (при этом пароль должен быть сложнее, чем «111» или «123», длиннее 6 символов, содержать буквы и цифры);
2. Убрать с рабочих мест листочки с паролями;
3. Автоматически блокировать компьютеры заставкой с паролем;
4. Ограничить доступ в кабинеты с компьютерами посторонних лиц без присмотра;
5. Установить файловый антивирус, регулярно обновлять базы;
6. Раз в месяц или чаще делать копии важных документов на компакт-диски или флеш-накопители.

РЕКОМЕНДУЕМЫЙ УРОВЕНЬ ЗАЩИТЫ

7. Разграничить права доступа к информационным системам организации, использовать аутентификацию по паролю, настроить ежедневное автоматическое архивирование;
8. Создать общее файловое пространство для документов организации в рамках локальной сети, разграничить права доступа и настроить регулярное автоматическое архивирование;
9. Установить комплексную защиту от вирусов и сетевых угроз;
10. Ограничить пользователям права на самостоятельную установку на компьютеры программного обеспечения;
11. Производить регулярную смену паролей.

ПРОДВИНУТЫЙ УРОВЕНЬ ЗАЩИТЫ

12. Настроить доменную аутентификацию пользователей;
13. Отключить использование съемных дисков и флешнакопителей;
14. Ограничить доступ сотрудников в сети Интернет к развлекательным порталам, социальным сетям, запретить скачивание программ, видео и музыки;
15. Повышать квалификацию сотрудников организации в области информационной безопасности;
16. Использовать лицензионное программное обеспечение и производить его регулярное обновление;
17. Разработать соглашение о неразглашении коммерческой тайны и конфиденциальной информации, подписать его всеми сотрудниками организации;
18. Разработать индивидуальный для организации комплекс мер по защите информации в соответствии с возможными моделями угроз.