Спорт

Шахматы

Состоялись заключительные соревнования городской спартакиады по шахматам. В соревнованиях приняли участие 13 команд, за которые играли лучшие шахматисты города Пинска. В составе нашей команды отлично зарекомендовал себя молодой работник нашего предприятия - кладовщик Дмитрий Артюх. Также честь автобусного парка защищали: водитель автомобильной колонны №1 Виталий Леонтюк и оператор диспетчерской движения АВ «Пинск» Татьяна Мирзоева.

В итоге ОАО «Пинский автобусный парк» занял место в середине таблицы.

Теннис

В спортивном зале гимназии №1 состоялись очередные соревнования городской спартакиады по настольному теннису. В соревнованиях приняло участие 11 команд.

Сборная команда нашего предприятия, поочередно победив команды КУПП ЖКХ г.Пинска,

ОАО «Строительный трест №2», Пинские тепловые сети, филиала «Камертон» ОАО «Интеграл», заняла в данной подгруппе первое место.

В другой подгруппе первое место занял многократный чемпион года – команда ЗАО ХК «Пинскдрев».

В финале наша команда в составе кассира билетного Рыжко Тамары, слесаря по ремонту автомобилей Терешко Андрея, каменщика Зубко Василия, проиграв со счетом 1:2, заняла второе место.

Вакансии

ОАО «Пинский автобусный парк» требуются на работу:
- кондуктор;
- водитель автобуса (категории «Д» или «ДЕ»);
- электрогазосварщик;
- инженер-механик;
- слесарь по ремонту автомобилей;
- автомаляр;

Телефон для справок **68-33-52.**

Объявление

18 декабря 2019 года в период времени с 15.00 до 16.30 руководством ОАО «Пинский автобусный парк» будет проводиться «**Горячая телефонная линия**».

Вопросы можно задать по номеру телефона **64-14-44**.

«Пинскгаз» информирует

В целях личной безопасности строго соблюдайте следующее:

- не допускайте к пользованию газовыми приборами и аппаратами: детей до 12 лет, лиц в нетрезвом состоянии, а также лиц, не прошедших инструктаж и не знающих правил безопасного пользования этими приборами;
- после окончания пользования газовыми приборами не оставляйте открытыми вентили баллонов (если баллон установлен внутри помещений), краны на подводящих газопроводах и газовых приборах;
- не пользуйтесь газовым оборудованием в случае его неисправности и при обнаружении запаха газа, а также при неисправности газопроводов, дымоходов, вентканалов, запорной аппаратуры (запорных кранов) и приборов автоматики;

- не оставляйте без присмотра работающие газовые приборы, кроме рассчитанных на непрерывную работу, оборудованных соответствующей автоматикой безопасности;
- не включайте конфорки газовой плиты и горелки духового шкафа для обогрева помещений - это опасно и может привести к отравлению угарным газом.

Запрещается проводить самовольное подключение и отключение газовых приборов и баллонов, перенос их на другое место, а также самостоятельную разборку и ремонт;

При обнаружении в помещении газа немедленно перекройте кран на опуске, откройте окна и двери и вызовите по телефону 104 аварийную газовую службу. До приезда аварийной службы и до устранения утечки газа не производите работ, связанных с огнем или искрообразованием (не включайте и не выключайте электроосвещение, не пользуйтесь газовыми или электрическими приборами, и не зажигайте огня).

Все интересующие вопросы можно задать по телефонам: 64-35-94; 64-95-92; 64-93-84.

ВЕСТНИК ОАО "ПИНСКИЙ АВТОБУСНЫЙ ПАРК"
Учредитель: ОАО "Пинский автобусный парк".
Редакционная коллегия: Савицкая Е.В., Богович В.В. Адрес: 225710, г. Пинск, ул. Брестская, 111. Тел. 8(0165) 68-33-52.Объем - 0,5 печ. л. Тираж 150 экз. Заказ №4693
Газета отпечатана с оригинал-макета редакции в коммунальном унитарном предприятии "Пинская региональная типография" главного управления идеологической работы и по делам молодежи Брестского облисполкома.

Издается с января 2008 года | ноябрь 2019 года | №11 (143)

ВЕСТНИК ОАО "ПИНСКИЙ АВТОБУСНЫЙ ПАРК"

Доска почета

За многолетний добросовестный труд в системе автомобильного транспорта, высокий уровень профессионализма и ответственности за выполнение порученной работы по итогам работы за 2018 год портрет заместителя главного бухгалтера Житинской Светланы Александровны занесен на Доску Почета ОАО «Пинский автобусный парк».

Житинская Светлана Александровна

Светлана Александровна родилась в г. Прилуки Черниговской области Украина. После окончания школы закончила Пинский учетно-кредитный техникум. В 2010 году закончила УО «Полесский государственный университет» по специальности «Экономика и управление на предприятии».

Всю свою трудовую деятельность она посвятила своей любимой профессии бухгалтера. Профессионал своего дела, Светлана Александровна пришла работать в автобусный парк с 6 февраля 2004 года на должность бухгалтера 1 категории. Постоянно повышает свой профессиональный уровень и в данный момент является заместителем главного бухгалтера.

Она проявила себя опытным специалистом высокой квалификации, профессионально применяет на практике познания в области финансов, бухучета, налогообложения и законодательства. Светлана Александровна прекрасно находит язык с партнерами и клиентами нашей организации. Все замечают ее вежливость и обходительность.

Отличительной чертой ее является коммуникабельность, умение сотрудничать с коллегами, готовность помочь и поделиться с ними опытом.

Светлана Александровна является активным участником общественной и спортивной жизни коллектива.

В свободное от работы время увлекается шитьем и вязанием.

Подготовка к зиме

Зима – строгий экзаменатор, который не прощает допущенных просчетов. Это прекрасно знают все, кто проходит испытания её холодами и прочими «сюрпризами». И, как всегда, каждый год комиссионно проводится обследование всех территорий и зданий предприятия для выявления недостатков, предотвращения аварийных ситуаций и понимать, какие будут затраты и в каком режиме нужно будет работать, чтобы быть готовыми к осенне-зимнему периоду.

Уже температура постепенно снижается, а это значит, что нужно подвести итоги о выполнении основных задач плана мероприятий по подготовке к осенне-зимнему периоду. Проведена работа по замене утеплителя на дверных проемах зданий, заменена запорная арматура на системе отопления АБК, проведена поверка приборов учета тепловой энергии, проверка системы отопления на диспетчерских пунктах и доливка теплоносителя до нужного уровня, частично заменена система отопления в авторемонтных мастерских филиала «Иваново», проведена работа по проверке, зачистке и гидравлическому испытанию систем отопления на предприятии, автовокзале «Пинск» и филиале «Иваново», выполнено испытание и проверка котлов в котельной, проверена и отрегулирована система подачи теплого воздуха в зданиях ТО-1, ТО-2, завершена работа по замене тепловой трассы на автовокзале «Пинск», что привело к сокращению тепловой потери на 60%, затрачено 39 000 руб., подписаны паспорта готовности к отопительному сезону.

С. ЗАБУРЧИК,
мастер ОГМ

Информационная безопасность

«Кто владеет информацией, тот владеет миром» (Н. Ротшильд).

Прогресс сделал компании зависимыми от информационных систем, а вместе с этим - уязвимыми к атакам хакеров, компьютерным вирусам, человеческому фактору в такой степени, что многие предприятия уже не могут чувствовать себя в безопасности. Вопрос информационной безопасности становится краеугольным камнем в деятельности организаций, но этот же прогресс предлагает решения, способные защитить данные от внешних посягательств.

Под информационной системой подразумевается совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. В ОАО «Пинский автобусный парк» используется много информационных систем, обеспечивающих решение обширного круга важных задач. Это такие участки, как:

- учет и обработка путевых листов;
- заправка автотранспорта топливом на АЗС;
- планирование работы водителей, кондукторов и транспорта;
- бухгалтерский и складской учет;
- планирование техобслуживания и ремонт техники;
- планирование и анализ расхода топлива, аккумуляторов, шин, других материалов;
- кадровый учет и начисление заработной платы;
- планировка маршрутов и графиков движения автотранспорта;
- GPS-мониторинг и анализ движения транспортных средств;
- интернет-сайт с информацией о расписании движения автобусов и услуг автопарка;
- web-сервис с информацией для пассажиров о движении автотранспорта в реальном времени.

Большинство этих систем тесно переплетены и зависят друг от друга. При сбое в одной начинает страдать и генерировать недостоверную информацию другая информационная система, что в результате может привести к серьёзным проблемам в работе автопарка.

Что такое информационная безопасность и почему системы ее обеспечения так важны? Обычно под ней понимают защищенность информации от преднамеренных или случайных действий, приводящих к нанесению ущерба самой компании или её клиентам. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Но из-за чего чаще всего возникают угрозы информационной безопасности?

1. Невнимательность и халатность сотрудников.

Угрозу информационной безопасности компании, как ни странно, могут представлять вполне лояльные сотрудники и не помышляющие о повреждении важных данных. Непредумышленный вред важной или конфиденциальной информации причиняется по простой халатности или неосведомленности работников. Всегда существует вероятность того, что кто-нибудь откроет фишинговое письмо и внедрит вирус с рабочего компьютера в локальную сеть и сервера компании.

Справочно: В августе 2019 года на корпоративную почту ОАО «Пинский автобусный парк» было получено вредоносное почтовое сообщение, которое мы опишем в качестве примера. Подобные письма приходят регулярно. Отправитель: Злата Журавлёва sergej@miecys.lt, Тема: Акт сверки четверг, Текст письма: «Направляю вложением документы 8е августа. Требуется проверить и вернуть скан документов, подписанного вами, на эту почту.», Вложение: файл «Документы 08.08.2019.001». Последние 3 цифры после точки маскируются для несведущего пользователя под какой-то номер документа, на самом деле таким образом именуются многотомные архивы RAR, ZIP, 7Z. После двойного щелчка «мышью» по такому «документу» открывается в программе-архиваторе архив с исполняемым файлом «Документы 08.08.2019.exe», щелкнув по которому можем запустить собственными руками для исполнения и заражения компьютера вредоносный процесс. Благодаря внимательности и осведомленности сотрудников, письмо было правильно идентифицировано и удалено.

Чтобы обойти антивирус, для распаковки архива может потребоваться пароль, который указан в письме. Если распаковать архив и запустить содержащийся в нём файл, на компьютер установится вредоносная программа, через которую злоумышленники смогут дистанционно управлять компьютером. Особенно опасно, если произошло заражение компьютера с установленной системой дистанционного банковского обслуживания (ДБО). Имея доступ к компьютеру с системой ДБО, злоумышленники могут узнать остатки на счетах, сформировать платёжные поручения на перевод денег на свой счет и отправить их в банк, подписав ЭЦП клиента. Кроме того, удалённый доступ к компьютеру позволяет похитить конфиденциальные документы клиента, установить шифровальщик-вымогатель или сделать его частью вредоносной сети для рассылки спама и организации атак.

Справочно: Летом 2019 года на одном из автотранспортных предприятий республики произошло заражение бухгалтерского компьютера с установленной системой ДБО. Бухгалтер оставила включенным компьютер без внимания с подключенным ключом с ЭЦП. Злоумышленник заблокировал экран и клавиатуру, сформировал платежное поручение на перевод денег на сумму более 70 000 руб. на счет одной из белорусских фирм, подписал платежку ЭЦП клиента, отправил её в банк. Деньги были перечислены. На следующий день при проверке выписки по счету кража была обнаружена. После обращения в правоохранительные органы деньги были найдены и возвращены владельцу.

Начало. Окончание на стр.3

Окончание. Начало на стр.2

2. Нелицензионное ПО.

Иногда руководители компаний пытаются сэкономить на покупке лицензионного ПО. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного ПО не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Также недоступны исправления, устраняющие обнаруженные бреши в системе безопасности, позволяющие злоумышленнику получить доступ к важной информации. Вместе с нелицензионным ПО есть вероятность получить вирусы, способные нанести вред системе компьютерной безопасности. По данным исследования Microsoft, в 7% изученных нелицензионных программ было найдено специальное программное обеспечение для кражи паролей и персональных данных.

3. Атаки на web-сайты.

DDoS, Distributed-Denial-of-Service - «распределенный отказ от обслуживания» - это поток ложных запросов от сотен тысяч географически распределенных хостов, которые блокируют выбранный ресурс. Недоступность или ухудшение качества работы публичных веб-сервисов в результате атак может продолжаться довольно длительное время, от нескольких часов до нескольких дней. Обычно подобные атаки используются в ходе конкурентной борьбы, шантажа компаний или для отвлечения внимания системных администраторов от неких противоправных действий вроде похищения денежных средств со счетов. По мнению специалистов именно кражи являются основным мотивом DDoS-атак. Мишенью злоумышленников чаще становятся сайты банков, в половине случаев (49%) были затронуты именно они. В 2016 году DDoS-атаки были зафиксированы в каждом четвертом банке (26%). Среди других финансовых структур вредному воздействию подверглось 22% компаний. Усредненный ущерб для кредитных организаций составил 1 172 000 долларов в расчете на банк.

Справочно: Ранее специалистами бюро АСУП ОАО «Пинский автобусный парк» ежедневно регистрировались многочисленные попытки атак на корпоративный сайт предприятия pinskap.by. В том числе это были атаки типа подбор пароля, DDoS-атаки, внедрение вредоносного кода (SQL Injection). С разработкой и внедрением в текущем году нового корпоративного сайта с поддержкой новейших стандартов информационной безопасности количество подобных атак сократилось практически до нуля.

4. Вирусы.

Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. Особенно активны стали так называемые вирусы-шифровальщики. Совсем недавно миллионы пользователей пострадали от атак вирусов WannaCry, Petya, Misha. Жертвой вирусной атаки можно стать, даже если не открывать подозрительные письма.

Справочно: WannaCry (в переводе означает «хочется плакать») - сетевой червь и вымогатель денежных средств. После заражения компьютера червь шифрует почти все файлы. Завершив процесс шифрования, выводит на экран окно с требованием перевести определённую сумму в биткойнах (эквивалентную 300$ США) на указанный кошелёк в течение 3 дней. Если выкуп не поступит своевременно, то его сумма будет автоматически удвоена. На 7 день, если WannaCry не будет удалён с инфицированной системы, зашифрованные файлы уничтожаются и информация теряется навсегда. Параллельно с шифрованием программа проводит сканирование произвольных адресов Интернета и локальной сети для последующего заражения новых компьютеров. Минимальная продолжительность времени между обнаружением уязвимого компьютера и полным его заражением составляет порядка 3 минут.

По информации Intel вирусом заразились 530 000 компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 200 странах мира. Распространение червя блокировало работу множества организаций по всему миру: больниц, аэропортов, банков, заводов и др. Общий ущерб компаний составил более 1 000 000 000 долларов.

Хотя количество угроз постоянно растет, появляются все новые и новые вирусы, разработчики средств защиты информации тоже не стоят на месте. На каждую угрозу разрабатывается новое защитное ПО или совершенствуется уже имеющееся.

Как защититься?

1. Будьте внимательней. Обращайте внимание на отправителя почты. Основная масса писем с вредоносным ПО содержит вложенные файлы форматов DOC, XLS, ZIP, RAR, 7Z, JS, SCR, MSI, CMD, BAT и EXE. Если в письме от незнакомого отправителя имеется пароль для доступа к такому файлу, не следует открывать вложенный файл и вводить указанную комбинацию букв и цифр. Файлы в формате JS, SCR, MSI, CMD, BAT и EXE не открывайте ни в коем случае! Не переходите по ссылкам в подозрительном письме.

2. Контролируйте наличие работающего антивируса и ежедневного обновления антивирусных баз.

3. Делайте регулярные резервные копии важных данных.

4. Извлекайте ключевые носители после завершения работы.

Итак, хоть защита информации в ОАО «Пинский автобусный парк» специалистами бюро АСУП осуществляется профессионально и комплексно, сразу по нескольким направлениям, информационная безопасность предприятия зависит от действий каждого пользователя на своем рабочем месте. В случае каких-либо подозрений во взломе ПК или личного аккаунта (электронной почты, программы 1С, интернет-банкинга и т.д.), проникновении вредоносного ПО, необходимо незамедлительно выключить компьютер и сообщить о происшествии в бюро АСУП, сотрудники которого всегда придут на помощь.

При создании статьи использовалась информация с сайтов wikipedia.org, microsoft.com, kp.ru, kaspersky.ru.

В. БОГОВИЧ,
начальник бюро АСУП