АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«ГОРОД САРАТОВ»

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ТРАНСПОРТНОЕ УПРАВЛЕНИЕ»

ПРИКАЗ

10.12.2018 № 583 **г. Саратов**

Об организации защиты информационной системы МКУ «Транспортное управление»

В целях организации защиты информационной системы и ее составляющих, защиты информации МКУ «Транспортное управление» – далее по тексту Управление, от угроз злонамеренного воздействия и несанкционированного доступа, а также во исполнение требований Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» приказываю:

1. Утвердить следующие инструкции:

- «Положение по организации политики информационной безопасности Управления» (приложение №1);
- «Положение по защите персональных данных» (приложение №2);
- «Инструкцию администраторов информационной безопасности Управления (приложение №3);
- «Инструкцию по организации антивирусной защиты в информационной системе Управления» (приложение №4);
- «Инструкцию по организации парольной защиты в информационной системе Управления» (приложение №5).
- «Инструкцию по организации защиты объектов информатизации Управления» (приложение №6);
- «Инструкцию о порядке работы с информационными ресурсами Управления для пользователей» (приложение №7);

2. Обязать сотрудников Управления неукоснительно соблюдать требования инструкций, а также требования государственных и ведомственных нормативных актов и документов по данным вопросам.
3. Персональную ответственность за соблюдение требований данных инструкций возложить на руководителей подразделений.
4. Разработку политики безопасности ее корректировку и организацию защиты компьютерной информационной системы возложить на начальника отдела АСУ и СНТ.
5. Организацию защиты персональных данных на бумажных носителях возложить на руководителя кадровой службы.
6. Координацию работ по организации защиты информационной системы возложить на заместителя директора Управления – Кобца А.В.
7. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **Е.А. Максимова**

Приложение №1

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ

1.Общие положения

Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Данное Положение предусматривает принятие мер в ответ на угрозы политике информационной безопасности Управления.

Положение не распространяется на порядок обеспечения безопасности сохранения служебной информации, содержащей сведения, составляющие государственную тайну, и ее носителей.

Положение распространяется исключительно на порядок обеспечения безопасности компьютерной сети и информации на электронных носителях.

Требования настоящего Положения обязательны для выполнения сотрудниками всех структурных подразделений Управления, использующих в своей работе ресурсы информационной системы».

1.1. Термины и определения

В данном Положении используются следующие понятия:

Объект информатизации Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Политика информационной безопасности (ИБ) – Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности. Комплекс организационных и программно-технических мер, обеспечивающих следующие параметры: доступность и целостность информации; конфиденциальность информации; невозможность отказа от совершенных действий; аутентичность электронных документов.

Несанкционированный доступ (НСД) - неправомочное получение, искажение или разрушения информации, вызов неисправностей и сбоев оборудования, программного обеспечения.

Законом «Об информации, информатизации и защите информации»определены следующие понятия:

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационные ресурсы (далее **ИР) -** отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках (базах) данных), других информационных системах (Интернет и т.п.).

Инцидент информационной безопасности - Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Автоматизированная информационная система (далее **АИС) -** организационно упорядоченная совокупность информационных ресурсов и информационных технологий, с использованием средств вычислительной техники и связи, реализующих информационные процессы.
Рабочая станция - компьютеры или удаленные терминалы сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов, администраторов).
Пользователи (потребители) – сотрудники, получившие допуск к работе с АИС в установленном порядке.
Имя пользователя – идентификатор пользователя АИС.
Пароль – аутентификатор, личный код пользователя, служащий для обеспечения режима конфиденциальности.
Сеанс пользователя (сеанс) - аутентифицированный вход в систему.

1.2. Краткий обзор

Организация защиты электронной информации в Управлении на начальника отдела информационных технологий.

Политика защиты информации разрабатывается начальник отдела автоматизированных систем и телекоммуникационных технологий под руководством заместителя директора, отвечающего за информационную безопасность Управления.

Защите подлежит информация, обрабатываемая информационной системой Управления, содержащая персональные данные и сведения, доступ к которым ограничен в соответствии с законодательством.

1.3. Угрозы политике информационной безопасности.

Основными угрозами являются:

1.3.1. нарушение работоспособности информационной системы, частей системы, отдельных программ;
1.3.2. утрата, модификация, потеря целостности информации;
1.3.3. хищение информации;
1.3.4. несанкционированное использование вычислительных ресурсов для организации майнинговых сетей, а также для организации хакерских атак и пр., как в личных целях, так и в целях нанесения ущерба интересам РФ

Перечисленные угрозы, могут вызываться программно – аппаратными сбоями, а также быть результатом ошибочных или преднамеренных действий должностных лиц, или сторонних злоумышленников, получивших доступ к системе. Воздействием компьютерных вирусов и программных закладок.

1.4. Методы защиты

1.4.1. Защита информационной системы и отдельных программ от нарушения работоспособности, вызванные программно – аппаратными сбоями осуществляется:

- соблюдением в серверном помещении и в рабочих помещениях рекомендованного в инструкциях по эксплуатации температурно – влажностного режима;
- обеспечением серверов и компьютеров источниками бесперебойного питания на случай аварийного выключения электроэнергии;
- формированием и хранением полного набора инсталляционных пакетов для оперативного восстановления работоспособности.

В случаях, если нарушение работоспособности информационной

системы или отдельных программ вызывается ошибочными или преднамеренными действиями должностных лиц, или сторонними злоумышленникам защита достигается:

- предотвращением несанкционированного доступа к активным элементам информационной системы – серверам, коммутаторам, маршрутизаторам, рабочим станциям и т. п. которые следует помещать в охраняемые помещения или (для коммутаторов, маршрутизаторов) в закрытые боксы;
- предотвращением, посредством программно аппаратных средств – межсетевых экранов, средств криптографической защиты, и т.п., несанкционированного доступа к системе по каналам передачи данных;
- организацией централизованной антивирусной защитой.

1.5. Защита информации от утраты, модификации (искажения), потери целостности хищения – неправомерного получения и использования достигается:

- организацией распределенного копирования;
- организацией централизованной антивирусной защитой;
- организацией централизованной системы распределения прав доступа к информационным ресурсам.

2. Действия в случае нарушения политики безопасности

Нарушение политики ИБ - случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) которое стало или могла стать причиной реализации угроз ИБ.

Значимость нарушения определяется причиненным или потенциальным ущербом.

По значимым нарушениям и нарушениям, имеющие признаки компьютерного преступления, назначается служебное расследование, проводимое экспертной комиссией под руководством заместителя руководителя Управления.

В состав комиссии в обязательном порядке входят начальник отдела автоматизированных систем управления и спутниковых навигационных систем, непосредственный начальник нарушителя, администратор информационной сети, сотрудники кадровой и юридической служб.

В случае необходимости к работе комиссии привлекаются эксперты из других подразделений.

На время проведения служебного расследования пользователь сети, совершивший нарушение, отключается от всех сервисов удаленного доступа и ресурсов информационной системы Управления.

Результат деятельности комиссии оформляется в виде экспертного заключения на имя руководителя Управления с предложениями по необходимым организационным выводам.

Контакты с правоохранительными органами, прессой и иными сторонними организациями определяются руководителем Управления.

2.1. Выработка решения о пресечении действий нарушителя

В Управление объявляются следующие стратегии решений о пресечении действий нарушителя:

- предпринимаются действия направленные на восстановление работоспособности информационной системы, а также

нормализации работы пользователей, злоумышленник не выявляется;

- предпринимаются действия направленные на восстановление работоспособности информационной системы, а также нормализации работы пользователей, злоумышленник выявляется для привлечения его к дисциплинарной ответственности;
- предпринимаются действия направленные на протоколирование действий злоумышленника с целью позволить ему продолжить свои действия и организовать судебное преследование.

Принятие решения о выборе стратегии возлагается на руководителя Управления. Наказание злоумышленника организуется в рамках действующего законодательства, компетентными правоохранительными органами.

2.2. Выработка процедур предупреждения нарушений безопасности

2.2.1. Защита информационных ресурсов Управления

Средств используемые для защиты информационных ресурсов:

- для предотвращения несанкционированного запуска компьютера произвести установку паролей на доступ к программному обеспечению BIOS (пароль администратора).
- для предотвращения несанкционированного допуска, к прошедшему идентификацию компьютеру, в отсутствие пользователя, установить пароль, на экранную заставку операционной системы;
- для предотвращения проникновения в информационную сеть Управления из других информационных сетей, использовать межсетевые экраны;
- использовать дополнительные средства для контроля от несанкционированного доступа к компьютерам, подключенным к информационной сети Управления.
- Для защиты от несанкционированного копирования информации с /на внешние носители на рабочих станциях отключить порты ввода – вывода.
- Для защиты от несанкционированной модификации и иных искажений программных продуктов установить антивирусных программных продуктов на всех компьютерах сети.
- В целях сохранения целостности или работоспособности баз данных информационной системы 1С Бухгалтерия и файловых массивов организовать их ежедневное копирование

2.2.2. Выявление возможных проблем

Выявление возможных проблем может производиться:

- собственными изысканиями в данной области;
- исходя из данных периодической печати и информационной сети Internet;
- на основе конференции и курсов повышения квалификации;
- силами сторонних организации или другими физическими лицами;

2.3. Выбор средств защиты

Выбор средств защиты осуществляется исходя из материальных возможностей Управления и в соответствии с нормативными актами Управления и ФСТЭК России (Федеральная служба по техническому и экспортному контролю).

2.3.1. **Физическая защита**

Для предотвращения несанкционированной физической модификации компьютера произвести опечатывание:

- корпуса системного блока компьютера;
- лицевой части компьютера - отсеки накопителей.

2.3.2. **Действия при подозрении на неавторизованную деятельность**

При подозрении на вторжение, компрометацию парольной защиты, сотрудник должен немедленно, довести до сведения своему непосредственному начальнику, в письменной форме.

После принятия решения руководителем Управления или начальником АСУ и СНТ организуются действия указанные в п. 2 настоящей Инструкции.

2.3.3. **Доведение политики безопасности**

Доведение политики безопасности до персонала следует проводить следующими методами:

- обучение пользователей;
- обучение администраторов;
- ознакомление с настоящим Руководством путем создания соответствующих, инструкций

на основе настоящего Руководства.

2.3.4. **Средства предупреждения нарушения политики безопасности**

В информационной сети Управления могут использоваться следующие средства по предупреждению возможности несанкционированного доступа:

- межсетевые экраны;
- ограничение сетевого доступа;
- система аутентификации;
- шифрование;
- электронно-цифровая подпись;
- а также другие аппаратные и процедурные ресурсы.

3. Типы процедур безопасности

3.1. **Проверка безопасности информационной системы**

Финансирование процедур безопасности планируется исходя из сметы Управления на предстоящий квартал.

Организовать проверку процедур безопасности один раз в год.

Проверка процедур предупреждения нарушений безопасности может производиться как собственными силами (АСУ и СНТ), так и специализированными сторонними организациями или другими физическими лицами.

3.1.1. **Процедура управления учетными записями**

Данная процедура описывается в «Инструкции администратора информационной безопасности Управления»

3.1.2. **Процедура конфигурационного управления**

Производить защиту от изменения конфигурации операционной системы, состава и системных настроек программного обеспечения, как штатными средствами, так и другими сертифицированными средствами.

Запретить пользователю, изменять конфигурацию операционной системы, состав и системные настройки программного обеспечения.

3.1.3. Процедура управления антивирусной защитой

Устанавливает политики постоянного антивирусного сканирования и график полной антивирусной проверки.

3.1.4. Процедура защиты от несанкционированного доступа к каналообразующему оборудованию, серверам, рабочим станциям

Запрещает несанкционированный доступ, модификацию и настройки оборудования

4. Реакция на нарушение

4.1. Эффективная реакция на инциденты

Для эффективной и своевременной реакции на инциденты организуется группа реагирования. Руководителем группы назначается начальник отдела информационных технологий.

Состав группы утверждается руководителем Управления по представлению руководителя группы реагирования.

Группой реагирования собирается следующая предварительная информация:

- возможные цели и побудительные мотивы инцидента;
- сохранность и восстанавливаемость данных, затронутых в ходе инцидента;
- поиск и наказание виновных, исходя из выбранной стратегии решения о пресечении действий нарушителя.

Группой реагирования предпринимаются следующие шаги:

- предотвращение развития вторжения и будущих инцидентов;
- предотвращение нежелательной огласки;
- минимизация урона, нанесенного вычислительным ресурсам;
- предотвращение повреждения информационной системы;
- защита конфиденциальной информации в соответствии с требованиями.

4.2. Оценка нарушения режима безопасности

Определяются следующие критерии определения масштаба последствий:

- стартовая точка инцидента;
- количество рабочих станций, вовлеченных в инцидент;
- находится ли под угрозой критически важная информация;
- затрагивает ли инцидент другие организации;
- потенциальный ущерб от инцидента;
- предполагаемое время ликвидации;
- ресурсы, необходимые для ликвидации инцидента;
- информированность других организации об инциденте.

4.3. Оповещение и извещение об инциденте

Во время обнаружения нарушения извещается следующие лица в следующем порядке:

- директор Управления;
- начальник отдела АСУ и СНТ (руководитель группы реагирования);
- другие лица и организации, по согласованию с директором Управления.

4.4. Организация устранения инцидента

Руководителем работ по устранению инцидента назначается руководитель

групп реагирования.

В его обязанности входят:

- организация ликвидации инцидента;
- организация восстановления последствий инцидента;
- координация действий сотрудников, задействованных на ликвидацию инцидента;
- организация сдерживания.

Для восстановления последствий инцидента происходящего проанализировать следующие моменты:

- когда произошел инцидент;
- дать точное определение инцидента;
- эффективность действия персонала;
- какая срочная информация потребовалась;
- эффективность получения информации;
- рассмотреть более эффективные действия персонала.

5. Выработка мер, предпринимаемых после нарушения

5.1. Актуализация процедур режима информационной безопасности

После устранения и регистрации инцидента связанного с НСД необходимо, произвести:

- анализ причин, приведших к инциденту, производится их документирование;
- анализ причин доводится до сведения руководства, которое принимает решение о реагировании на происшедшее.

Пересмотр информационных ресурсов, подлежащих защите, происходит:

- по мере их возникновения;
- указания вышестоящей организации;
- экспертных оценок сторонних специализированных организации.

При возникновение новых информационных ресурсов производится новый анализ рисков, о чем составляется дополнение к данному Положению.

5.2. Устранение выявленных слабостей

После устранения и регистрации инцидента связанного с НСД на основе экспертных оценок необходимо произвести оценку ущерба.

Оценка ущерба производятся соответствующими организациями, а в случае принятия стратегии по невыявлению злоумышленника производится самостоятельно.

Приложение №2

ПОЛОЖЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ № 197-ФЗ от 30.12.2001 г., Федеральным законом РФ "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27.07.2006 г., Федеральным законом РФ "О персональных данных» № 152-ФЗ от 27.07.2006 г., Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г. и другими нормативными правовыми актами.

1.2. Настоящее Положение определяет порядок обработки персональных данных работников Управления и гарантии конфиденциальности сведений, предоставляемых работником работодателю.

1.3. Персональные данные работника являются конфиденциальной информацией.

2. . Понятие и состав персональных данных работника

Персональные данные работника - это необходимая работодателю в связи с трудовыми отношениями информация о конкретном сотруднике. К персональным данным работника относятся:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- данные о семейном положении;
- паспортные данные работника;
- данные об образовании работника, наличии специальных знаний или подготовки;
- данные о профессии, специальности работника;
- сведения о доходах работника;
- данные о членах семьи работника;
- данные о месте жительства, почтовый адрес, телефон работника, а также членов его семьи;
- данные, содержащиеся в трудовой книжке работника и его личном деле, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет, сведения о медицинском страховании;
- данные, содержащиеся в документах воинского учета (при их наличии);
- иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

3. Обработка персональных данных работника

3.1. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника. Обработка персональных данных работника осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности работника, контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами,

предусмотренными законодательством РФ и актами работодателя.

3.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.3. На основании норм Трудового кодекса РФ (ст. 86), а также исходя из положений п. 2 ст. 6 Федерального закона №152-ФЗ "О персональных данных", обработка персональных данных осуществляется работодателем без письменного согласия работника, за исключением случаев, предусмотренных федеральным законом.

3.4. Все персональные данные о работнике работодатель может и должен получить от него самого.

3.5. Работник обязан предоставлять работодателю достоверные сведения о себе и своевременно сообщать ему об изменении своих персональных данных в течение 30 дней. Работодатель имеет право проверять достоверность сведений, предоставленных работником, сверяя данные, предоставленные работником, с имеющимися у работника документами.

3.6. В случаях, когда работодатель может получить необходимые персональные данные работника только у третьего лица, работодатель должен уведомить об этом работника и получить от него письменное согласие по установленной форме (Приложение 2.1).

Работодатель обязан сообщить работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение. Персональные данные работника хранятся в кадровой службе в личном деле работника. Личные дела хранятся в бумажном виде в папках и находятся в сейфе.

Персональные данные работника в кадровой службе хранятся также в электронном виде в базе данных. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечиваются системой паролей. Пароли устанавливаются руководителем кадровой службы и сообщаются индивидуально сотрудникам кадровой службы, имеющим доступ к персональным данным работников.

Примечание: Хранение персональных данных работников в бухгалтерии и иных структурных подразделениях работодателя, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке исключающим к ним доступ третьих лиц.

3.7. Сотрудник работодателя, имеющий доступ к персональным данным работников в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные работника, исключающее доступ к ним третьих лиц. В отсутствие сотрудника на

его рабочем месте не должно быть документов, содержащих персональные данные работников (соблюдение "политики чистых столов").

- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные работников лицу, на которое локальным актом Организации (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

***Примечание*:** В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию руководителя структурного подразделения.

При увольнении сотрудника, имеющего доступ к персональным данным работников, документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию руководителя структурного подразделения.

3.8. Доступ к персональным данным работника имеют сотрудники работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей (Приложение 2.2).

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией руководителя Управления, доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей сотрудников, имеющих доступ к персональным данным работника Управления, и которым они необходимы в связи с исполнением трудовых обязанностей.

3.9. В случае если работодателю оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным работников Управления, то соответствующие данные предоставляются работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника.

3.10. Процедура оформления доступа к персональным данным работника включает в себя:

- ознакомление работника под роспись с настоящим Положением. *Примечание*: При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление работника под роспись.
- истребование с сотрудника (за исключением руководителя Управления) письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки, подготовленного по установленной форме (Приложение 2.3).

3.11. Сотрудники работодателя, имеющие доступ к персональным данным работников, имеют право получать только те персональные данные работника, которые необходимы им для выполнения конкретных трудовых функций.

3.12. Допуск к персональным данным работников без специального разрешения имеют работники, занимающие в Управления следующие должности:

- руководитель Управления;
- заместитель руководителя Управления;
- главный бухгалтер;
- работники кадровой службы;
- работники юридической службы;
- администраторы информационной безопасности
- начальники служб и отделов в отношении персональных данных работников, числящихся в соответствующих структурных подразделениях.

3.13. Допуск к персональным данным работника других сотрудников работодателя, не имеющих надлежащим образом оформленного допуска, запрещается.

3.14. Работник имеет право на свободный допуск к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Работник имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

3.15. Кадровая служба вправе передавать персональные данные работника в бухгалтерию и иные структурные подразделения, в случае необходимости исполнения сотрудниками соответствующих структурных подразделений своих трудовых обязанностей.

При передаче персональных данных работника, сотрудники кадровой службы предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

3.16. Передача (обмен и т.д.) персональных данных между подразделениями работодателя осуществляется только между сотрудниками, имеющими допуск к персональным данным работников.

3.17. Передача персональных данных работника третьим лицам осуществляется только с письменного согласия работника, которое оформляется по установленной форме (Приложение 2.4) и должно включать в себя:

- фамилию, имя, отчество, адрес работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес работодателя, получающего согласие работника;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие работник;
- срок, в течение которого действует согласие, а также порядок его отзыва.

***Примечание*:** Согласия работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника; когда третьи лица оказывают услуги работодателю на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

3.18. Не допускается передача персональных данных работника в коммерческих целях без его письменного согласия, оформленного по установленной форме (Приложение 2.5).

3.19. Сотрудники работодателя, передающие персональные данные работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме (Приложение 2.6), и должен содержать следующие условия: уведомление лица,

получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

3.20. предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

3.21. Передача документов (иных материальных носителей), содержащих персональные данные работников, осуществляется при наличии у лица, уполномоченного на их получение:

3.22. договора на оказание услуг Управления;

3.23. соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных работника;

3.24. письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

3.25. Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных работника Управления несет работник, а также руководитель структурного подразделения, осуществляющего передачу персональных данных работника третьим лицам.

3.26. Представителю работника (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя работника;
- письменного заявления работника, написанного в присутствии сотрудника отдела кадров работодателя (если заявление написано работником не в присутствии сотрудника отдела кадров, то оно должно быть нотариально заверено).
- Доверенности и заявления хранятся в кадровой службе в личном деле работника.

3.27. Предоставление персональных данных работника государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

3.28. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника, за исключением случаев, когда передача персональных данных работника без его согласия допускается действующим законодательством РФ.

3.29. Документы, содержащие персональные данные работника, могут быть отправлены через организацию федеральной почтовой связи.

3.30. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем.

3.31. Общую организацию защиты персональных данных работников осуществляет руководитель кадровой службы, обеспечивающий:

- ознакомление сотрудника под роспись с настоящим Положением;
- ознакомление сотрудника под роспись с иными нормативными актами (приказы, распоряжения, инструкции и т.п.), регулирующими обработку и защиту персональных данных работника;
- истребование с сотрудников (за исключением лиц, указанных в пункте 3.13 настоящего Положения) письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил

их обработки.

4. Общий контроль за соблюдением сотрудниками работодателя мер по защите персональных данных работника.

4.1. Организацию и контроль защиты персональных данных работников служб и отделов Управления, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

4.2. Защите подлежат:

- информация о персональных данных работника;
- документы, содержащие персональные данные работника;
- персональные данные, содержащиеся на электронных носителях.

4.3. Защита сведений, хранящихся в электронных базах данных работодателя, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

5. Заключительные положения

5.1. Иные права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных работника, определяются также должностными инструкциями.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

5.3. Разглашение персональных данных работника Управления (передача их посторонним лицам, в том числе, работникам Управления, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные работника, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Управления, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания - замечания, выговора, увольнения.

5.4. Сотрудники, имеющие доступ к персональным данным работника и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба работодателю (п.7 ст. 243 Трудового кодекса РФ).

5.5. Сотрудники, имеющие доступ к персональным данным работника, виновные в незаконном разглашении или использовании персональных данных работников работодателя без согласия работников из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ

Приложение №3

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННОЙ СИТЕМЫ УПРАВЛЕНИЯ

Инструкция предназначена, и обязательна для исполнения администраторами информационной системы, администраторами баз данных – далее по тексту Администраторами.

Администраторы назначаются приказом директора из числа штатных сотрудников Управления.

1. Обязанности администратора информационной безопасности локальной вычислительной сети

1.1. Администратор информационной безопасности локальной вычислительной сети обязан:

1.1.1. фиксировать все инциденты и письменно докладывать о них непосредственному руководителю.

1.1.2. сопровождать учетные записи пользователей:

- корректировать список пользователей;
- устанавливать и изменять права и привилегии пользователей по данным, предоставленным начальниками служб и отделов и утвержденных директором Управления;
- вводить ограничения на регистрацию в сети.
- оперативно реагировать на попытки НСД и информировать об этом руководителя подразделения;
- осуществлять оперативный контроль действий пользователей и событий, связанных с доступом к информационным ресурсам Управления в целях выявления попыток НСД и нарушений установленной технологии обработки информации ограниченного распространения;
- анализировать журналы событий;

1.1.3. сопровождать антивирусное программное обеспечение

- регулярно контролировать работоспособность антивирусного программного обеспечения на всех компьютерах ЛВС Управления;
- контролировать график обновлений антивирусных баз;
- выявлять наличие компьютерных вирусов и программных закладок на серверах и рабочих станциях и проводить их обезвреживание. Выявлять и обезвреживать источники заражения;

1.1.4. производить и периодически контролировать, в соответствии с утвержденными групповыми политиками, настройки серверов, межсетевых экранов

1.1.5. регулярно, в соответствии с утвержденным графиком осуществлять резервное копирование баз данных и иной значимой информации

1.1.6. оказывать практическую помощь пользователям в применении программного обеспечения.

2. Администратор имеет право

при обнаружении несанкционированных действий поступать в соответствии с п.2.1 «Положения по организации политики информационной безопасности

Управления»

3. Ответственность

3.1. Администратор несет персональную ответственность за сохранность охраняемой информации.

3.2. За разглашение, хищение информации, доступ к которой он получил в процессе производственной деятельности, администратор несет ответственность в соответствии с законодательством РФ

Приложение №4

ИНСТРУКЦИЯ ОБ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

1. Общие положения

1.2. Настоящая Инструкция разработана в целях защиты информационной системы Управления, от угроз несанкционированного копирования (хищения), модификации и разрушения информации, а также нарушения работы информационной системы при воздействии вредоносных программ.

2. . Принципы антивирусной политики информационной системы Управления

2.1. Политика, схема и график централизованной антивирусной защиты разрабатываются начальником отдела АСУ СНТ и утверждаются директором Управления.

2.2. Все устройства ввода - вывода информации с отчуждаемых носителей должны быть заблокированы, за исключением рабочих мест пользователей, допущенным к работе с отчуждаемыми носителями по распоряжению директора.

2.3. В целях реализация политики информационной безопасности Управления на администратора информационной безопасности возлагаются следующие функции:

2.3.1. общий контроль соблюдения работниками политик информационной безопасности;

2.3.2. создание и контроль исполнения задач постоянного антивирусного сканирования на рабочих станциях и серверах в режиме реального времени;

2.3.3. создание и контроль исполнения задач полного антивирусного дискового сканирования;

2.3.4. создание и контроль исполнения **пополнения и обновления** антивирусного ПО;

2.4. Установка и копирование на жесткие диски рабочих станций, а также использование в сети Управления любых файлов непроизводственного назначения производится исключительно администратором информационной безопасности.

3. Правила работы и обязанности сотрудников по антивирусной защите компьютерной сети

3.1. Ввод информации с магнитных, оптических, магнитооптических съемных носителей или накопителей всех видов, при возникновении служебной необходимости, должен осуществляться только сотрудниками, имеющими допуск к работе с устройствами ввода вывода информации с отчуждаемых носителей. Данное положение не предусматривает каких-либо исключений.

3.2. Копирование любой информации, переносимой с помощью съемных магнитных, оптических, магнитооптических носителей и USB накопителей всех видов, должно производиться только после проведения процедуры антивирусного контроля отчуждаемого носителя. Данное положение не предусматривает каких-либо исключений.

3.3. В случае появления подозрений на наличие вирусов в компьютерной сети Управления сотрудники должны немедленно ставить в известность администратора компьютерной сети, либо его непосредственного начальника.
3.4. Все факты модификации и разрушения данных на серверах или рабочих станциях Управления, а также заражение их вирусами, классифицируются как «Значимые нарушения информационной безопасности» и должны анализироваться через процедуру служебного расследования

Приложение №4

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

1. Общие положения

1.1 Настоящая Инструкция разработана для предотвращения несанкционированного доступа к ресурсам информационной системы Управления в целях не допущения утечки конфиденциальной информации, а также несанкционированной модификации или уничтожения данных.

1.2 Операционные системы рабочих станций, включенных в компьютерную сеть Управления, должны иметь возможность настройки, исключающей возможность просмотра одного или нескольких последних паролей. Данное положение действует без исключений.

1.3 Операционные системы серверов, локальной вычислительной сети Управления должны настраиваться таким образом, чтобы блокировать вход в сеть после троекратной ошибки в наборе пароля. Данное положение действует без исключений.

2. Порядок заведения и регистрации паролей доступа пользователей

2.1 При введении нового пользователя администратор локальной вычислительной сети должен назначить для него однократный пароль доступа к ресурсам локальной вычислительной сети.

2.2 Пользователь обязан заменить однократный пароль - личным при первом же входе в компьютерную сеть.

2.3 При регистрации доступа пользователя к автоматизированным информационным системам «1С бухгалтерия» и «1С бухгалтерия и кадры», администратор баз данных должен назначить для него однократный пароль доступа.

2.4 Пользователь обязан заменить однократный пароль - личным при первом же обращении к ресурсам.

3. Период действия пароля пользователей

3.1 Периодичность смены парольной информации задается администратором локальной вычислительной сети централизованно, для всех пользователей.

3.2 Период действия паролей для входа в компьютерную сеть не должен превышать 45 суток. Данное положение действует без исключений. При сообщении компьютерной системы об окончании срока действия личного пароля пользователь обязан заменить его на новый, ранее не применявшийся.

4. Ограничение доступа к информации о паролях

4.1 Операционная система должна быть настроена таким образом, чтобы исключить возможность ознакомления с парольной информацией любого из пользователей, включая администратора локальной вычислительной сети. Данное положение действует без исключений.

5. Принципы выбора и формирования личных паролей

5.1 Категорически запрещается использование в качестве пароля легко

угадываемых последовательностей символов типа: номеров телефонов, имен своих и родственников и т.п.

5.2 В качестве парольной информации следует выбирать последовательность букв, цифр и служебных символов длиной не менее шести знаков.

5.3 В пароле, кроме буквенных последовательностей, рекомендуется использовать не менее двух цифр.

5.4 Рекомендуется использование в части парольной информации русских слов, набираемых в латинском регистре (без переключения клавиатуры). Пример (Слово ЮРИСТ будет выглядеть как .HBCN).

6. Правила работы и обязанности сотрудников по использованию и сохранению в тайне личного пароля

6.1 Информация о паролях пользователей является конфиденциальной информацией, предназначенной для идентификации и допуска каждого конкретного пользователя к ресурсам локальной вычислительной.

6.2 Администраторам сети категорически запрещается использование административного бюджета при повседневной деятельности, не связанной с административными функциями. Для этой цели администратору локальной вычислительной сети должен выделяться бюджет с правами пользователя.

6.3 Набор личного пароля следует проводить, исключив возможность его компрометации.

6.4 При оставлении рабочего места необходимо использовать функцию «временной блокировки».

6.5 Запрещается:

6.5.1 Умышленное или неумышленное ознакомление с парольной информацией сотрудников Учреждения и посторонних лиц, независимо от их должности:

6.5.2 Передача личного пароля сослуживцам или руководителям подразделения;

6.5.3 Запись личного пароля доступа на бумагу и хранение его в потенциально доступном для ознакомления посторонними и другими сотрудниками месте;

6.5.4 Вход в локальную вычислительную сеть с использованием чужих идентификаторов доступа;

6.5.5 Оставлять без присмотра рабочее место с открытой пользовательской сессией;

6.6 В случае утраты пароля, сотрудники должны сообщить об этом администратору локальной вычислительной сети или администратору баз данных и получить у них новый пароль для однократного доступа.

6.7 В случае подозрения о раскрытии пароля, сотрудники обязаны произвести экстренную замену личного пароля и незамедлительно поставить об этом в известность администратора информационной безопасности для исключения возможности утечки информации.

6.8 Сотрудники Управления обязаны незамедлительно докладывать администратору информационной безопасности о всех замеченных нарушениях, связанных с доступом в компьютерную сеть и информационную систему регистрации.

6.9 Любые некорректные действия сотрудников и посторонних лиц, связанные с доступом в компьютерную сеть, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.

Приложение № 5

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ УПРАВЛЕНИЯ

1. Общие положения

Настоящая Инструкция разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в целях защиты информационной системы Управления, от угроз несанкционированного использования вычислительных ресурсов для организации майнинговых сетей, а также для организации хакерских атак и пр., как в личных целях, так и в целях нанесения ущерба интересам РФ.

2. Принципы защиты помещений, где проводится обработка информации

2.1. Ответственными за соблюдение режима безопасности помещений назначаются начальники служб и отделов, работники которых занимают данные помещения.

2.2. Ответственные разрабатывают и утверждают график дежурств по помещению.

2.3. Дежурный по помещению прибывает на работу заблаговременно, получает у диспетчера ключ, о чем делается запись в журнале. Убедившись в целостности пломбы, открывает помещение.

2.4. По окончании рабочего дня дежурный, убедившись, что в помещении никого не осталось закрывает его на ключ и пломбирует личной пломбой. Ключ сдается дежурному диспетчеру, о чем делается запись в журнале.

2.5. В случае, если обнаружено нарушение пломбы дежурный обязан доложить о данном факте начальнику своего отдела, службы.

3. Хранение документов на бумажных носителях, содержащих персональные данные и иную информацию, защищаемую в соответствии с законодательством.

3.1. Хранение документов на бумажных носителях осуществляется в закрываемых на ключ металлических шкафах.

3.2. Ключи от шкафов находится у главного бухгалтера и руководителя кадровой службы соответственно.

4. Принципы защиты компонентов информационной системы Управления

4.1. Схема локальной сети, порядок ввода в эксплуатацию коммутаторов, маршрутизаторов, серверов и компьютеров разрабатываются начальником отдела АСУ СНТ и утверждаются директором Управления.

4.2. Подключения локальной сети, собранной по утвержденной схеме отражаются в кроссовых таблицах

4.3. Элементы локальной сети должны размещаться в местах, исключающих доступ к ним посторонним:

4.3.1. Серверы – в закрытых, специально выделенных помещениях, ключ от которого хранится у дежурного и выдается под роспись согласно утвержденного списка;

4.3.2. Маршрутизаторы, коммутаторы в закрываемых монтажных шкафах, ключи от которых хранятся у начальника отдела АСУ и СНТ;

4.3.3. Компьютеры на рабочих местах размещаются в закрываемых

помещениях, ключ от которых хранится у дежурного и выдается под роспись согласно утвержденного списка (Приложение 6.1);

4.4. Ввод в эксплуатацию элементов локальной сети производится в следующем порядке:

4.4.1. маршрутизаторы, настраиваемые коммутаторы вводятся в эксплуатацию после проведения настроек в соответствии с требованиями «Положения по организации политики информационной безопасности Управления». Настройки защищаются средствами парольной защиты

4.4.2. компьютеры – серверы и рабочие станции вводятся в эксплуатацию после визуального внутреннего осмотра с последующим составлением паспорта устройства, в котором отражается «наименование элемента» «изготовитель», «модель», «технические характеристики», серийный номер. Все устройства опечатываются.

4.4.3. новые рабочие места вводятся в эксплуатацию после составления паспорта рабочего места. В паспорт рабочего места вносятся сведения о периферии компьютера, установленном программном обеспечении и его настройках

4.4.4. Все паспорта хранятся у начальника отдела АСУ и СНТ

Приложение №6

ИНСТРУКЦИЯ О ПОРЯДКЕ РАБОТЫ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ (для пользователей)

Настоящая инструкция разработана в соответствии Трудовым Кодексом РФ (далее ТК РФ), федеральным законом 27 июля 2006 г. N 149-ФЗ «Об информации, информатизации и защите информации», «Частной моделью угроз безопасности персональных данных сотрудников МКУ «Транспортное управление» и данных, содержащих информацию, доступ к которой ограничен законодательством в информационной системе МКУ «Транспортное управление».

1. Общие положения

1.1. Инструкция определяет правила работы в информационной системе Управления. Положения Инструкции обязательны для исполнения всеми пользователями АИС Предприятия.

1.2. Приостановка и прекращение допуска к работе с АИС, а также назначение и изменение прав доступа к ее ресурсам осуществляется на основании служебной записки, утвержденной директором Управления (Приложение 7.1).

2. Порядок работы в локальной информационной системе

2.1. Использовать ресурсы АИС Предприятия в строгом соответствии с должностными обязанностями.

2.2. Перед началом работы проверять целостность защитных наклеек (стикеров), пломб, установленных на системных блоках.

2.3. Не допускать посторонних к работе на автоматизированном рабочем месте.

2.4. Предпринимать меры по предотвращению использования открытого сеанса другими пользователями, для чего блокировать рабочую станцию при кратковременном оставлении рабочего места (Ctrl+Alt+Del; «Блокировка»; «Да») и выходить из системы при завершении сеанса работы («Пуск»; «Завершение работы»; «Завершение сеанса «ИМЯ»; «Да»). По окончании работы завершить работу системы («Пуск»; «Завершение работы»; «Да»), обесточить рабочую станцию.

2.5. Обрабатывать информацию, содержащую персональные данные, только на специализированных рабочих местах в установленном порядке.

2.6. Хранить электронную информацию, относящуюся к деятельности подразделения только в специально отведенных каталогах («папках»), указанных непосредственным руководителем.

3. Правила работы с ресурсами Интернет и внешней электронной почтой

3.1. Интернет и внешняя электронная почта предназначены для оперативного доступа к новостной, справочной и технической информации, а также для оперативного обмена информацией.

3.2. Допуск и право доступа к информационным ресурсам Интернет и внешней электронной почте предоставляется в соответствии с п. 1.2 настоящей инструкции.

3.3. Весь Интернет трафик Предприятия (трафик - количество принятой и переданной информации или время пользования ресурсами Интернет) автоматически регистрируется системными журналами, в них фиксируется: имя пользователя,

количество переданной и принятой пользователем информации, Интернет контент, компьютер с которого осуществлялся доступ.

3.4. Руководитель структурного подразделения может письменно запросить у начальника отдела АСУ и СНТ отчет о трафике работников своего подразделения, допущенных к работе с ресурсами Интернет.

3.5. При работе с электронной почтой сотрудники должны удалять корреспонденцию без обратного адреса или с непонятным обратным адресом (набором символов или цифр), а также пришедшую с неизвестных адресов.

4. Пользователю запрещается:

4.1. Использовать имя и пароли другого пользователя, а также использовать активные сеансы других пользователей.

4.2. Компрометировать парольную защиту: разглашать пароль – аутентификатор, предпринимать попытки его подбора или программного «взлома».

4.3. Вносить в базы данных и технологические документы заведомо недостоверную информацию.

4.4. Допускать посторонних на автоматизированное рабочее место.

4.5. Отключать антивирусную защиту

4.6. Посещать сайты не связанные с исполнением функциональных обязанностей:

4.6.1. Развлекательные.

4.6.2. Игровые.

4.6.3. Содержащие порнографический и эротический контент.

4.6.4. Социальные сети.

4.6.5. Фильмотеки и пр.

4.7. Самовольно размещать в Интернет изданиях и форумах информацию о предприятии и его сотрудниках.

4.8. Предпринимать попытки:

4.8.1. доступа к информационным ресурсам Управления, не относящимся к его компетенции;

4.8.2. модификации системных ресурсов, и настроек, в том числе: системного времени, задач резервного копирования, подключений к сети предприятия, настроек антивирусной защиты и пр.;

4.8.3. сокрытия файлов и каталогов.

4.8.4. подключения к сети Internet и использования его ресурсов, в обход существующих правил;

4.8.5. Оставлять автоматизированное рабочее место без принятия мер безопасности (установки блокировки, завершения сеанса или выхода из системы).

4.8.6. устанавливать программное обеспечение;

4.8.7. производить работы на автоматизированных рабочих местах в нерабочее время и на автоматизированных рабочих местах других структурных подразделений;

4.8.8. предпринимать попытки запуска программ и открытия файлов, не относящиеся к программному обеспечению, необходимому для выполнения им служебных обязанностей;

4.8.9. применять системные средства защиты файлов и каталогов (шифрование);

4.8.10. подключать и переключать периферийные устройства (сканеры,

принтеры, модемы и пр.);

4.8.11. производить подключение системных блоков к сетевым коммуникациям предприятия;

4.8.12. нарушать целостность защитных наклеек, пломб, установленных на системных блоках;

4.8.13. вскрывать системные блоки и изменять их конфигурацию;

4.8.14. вскрывать защитные короба сетевых коммуникаций и коммутационные шкафы.

5. Ответственность за нарушение данной инструкции.

Нарушение настоящей инструкции влечет последствия в соответствии с п. 5 «Положения по организации политики информационной безопасности Управления»