ГОРОДСКОЙ ОКРУГ УРАЙ
Ханты-Мансийского автономного округа - Югры

АДМИНИСТРАЦИЯ ГОРОДА УРАЙ
ПОСТАНОВЛЕНИЕ

от 26.04.2022 № 968

Об утверждении документов
по информационной безопасности

В целях обеспечения безопасности информации, обрабатываемой в локально-вычислительной сети администрации города Урай, предотвращения ее разрушения, потери от неквалифицированных действий пользователей, внешних угроз, повышения эффективности использования вычислительной техники, компьютерных сетей и информационных ресурсов, повышения ответственности сотрудников органов местного самоуправления города Урай и в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1. Утвердить документы по информационной безопасности:

1) Порядок использования паролей согласно приложению 1;

2) Порядок использования сети «Интернет» согласно приложению 2;

3) Порядок использования электронной почты согласно приложению 3;

4) Порядок организации антивирусной защиты согласно приложению 4;

5) Порядок проведения технического обслуживания согласно приложению 5;

6) Порядок управления доступом к объектам информатизации согласно приложению 6;

7) Порядок физического доступа на объекты информатизации согласно приложению 7;

8) Порядок инвентаризации информационных активов согласно приложению 8;

9) Инструкцию по организации резервного копирования (восстановления) данных, обрабатываемых в информационных системах, согласно приложению 9;

10) Порядок управления инцидентами по информационной безопасности согласно приложению 10;

11) Порядок работы с криптосредствами и электронной подписью согласно приложению 11;

12) Инструкцию пользователя по работе с объектами информатизации согласно приложению 12;

13) Инструкцию по работе с машинными носителями информации в информационных системах согласно приложению 13;

14) Инструкцию по использованию программных и аппаратных средств защиты информации согласно приложению 14.

2. Назначить ответственным за организацию работ по защите информации в органах местного самоуправления города Урай начальника управления по информационным технологиям и связи администрации города Урай С.А.Осипову.

3. Назначить администратором информационной безопасности органов местного самоуправления города Урай, работающих в локально-вычислительной сети администрации города Урай, специалиста-эксперта отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай Ю.А.Овечкина.

4. Назначить ответственным за эксплуатацию средств криптографической защиты информации администрации города Урай консультанта отдела по информационным ресурсам управления по информационным технологиям и связи администрации города Урай Р.Р.Галиахметова.

5. Считать утратившими силу постановления администрации города Урай:

1) от 29.07.2016 №2278 «Об утверждении порядков по информационной безопасности»;

2) от 13.09.2017 №2638 «О внесении изменений в постановление от 29.07.2016 №2278 «Об утверждении документов по информационной безопасности».

6. Управлению по информационным технологиям и связи администрации города Урай (С.А. Осипова) обеспечить ознакомление с постановлением пользователей локально-вычислительной сети администрации города Урай.

7. Контроль за выполнением постановления возложить на заместителя главы города Урай О.Н.Хотинецкого.

Глава города Урай Т.Р.Закирзянов

Приложение 1 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок использования паролей

1. Назначение и область действия.

Порядок использования паролей (далее - Порядок) определяет основные правила обращения с паролями, используемыми для доступа к информационным системам и ресурсам (далее – ресурсы) органов местного самоуправления города Урай.

Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

Настоящий порядок должен соблюдаться в той мере, в которой это допускается техническими возможностями самого ресурса.

2. Основные требования.

Доступ к ресурсам должен производиться с использованием персональных учетных записей и периодически сменяемых буквенно - цифровых паролей, удовлетворяющих следующим требованиям:

1) пароль содержит не менее восьми символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

3) не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т.п.), в том числе набранным в другой раскладке клавиатуры;

4) при смене пароля новое значение должно отличаться от предыдущих.

Временный пароль, создаваемый администратором информационной безопасности при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем при первом обращении к ресурсу.

Пароли, предустановленные производителем, должны сменяться до начала эксплуатации ресурсов.

Смена пароля должна производиться не реже одного раза в три месяца или при обнаружении фактов, указывающих на его возможную компрометацию, а в отношении административных учетных записей - также при смене лица, выполняющего административные функции.

В зависимости от критичности ресурса, его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение и другие обстоятельства) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с ресурсом на основании письменного указания непосредственного руководителя органа (структурного подразделения).

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности.

В случае компрометации (утеря, передача другому лицу) личного пароля, пользователь обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

Пароли ключевых учетных записей критически важных ресурсов должны сохраняться в запечатанном конверте в сейфе начальника отдела по защите информации и связи управления по информационным технологиям и связи администрации города Урай или у руководителя органа местного самоуправления города Урай - владельца соответствующего ресурса.

3. Запрещается:

1) сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем ресурсов);

2) сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

3) использовать учетные записи других лиц;

4) использовать вне органов местного самоуправления города Урай пароли, совпадающие с паролями доступа к его ресурсам.

4. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 2 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок использования сети «Интернет»

1. Назначение и область действия.

Порядок использования сети «Интернет» (далее - Порядок) определяет основные требования по защите информации от угроз, связанных с использованием сети «Интернет».

Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Основные требования.

Использование сети «Интернет» должно быть санкционировано в соответствии с действующей процедурой предоставления доступа к информационным ресурсам и локально-вычислительной сети органов местного самоуправления города Урай.

Использование сети «Интернет» должно осуществляться только для выполнения функциональных обязанностей работника.

Конфиденциальная информация, передаваемая с использованием сети «Интернет», должна быть защищена от несанкционированного просмотра или модификации.

Содержание и объем информации, передаваемой или принимаемой с использованием сети «Интернет», могут ограничиваться администратором информационной безопасности.

Управление по информационным технологиям и связи администрации города Урай оставляет за собой право мониторинга использования сети «Интернет» с целью соблюдения основных требований Порядка.

Состав, архитектура и конфигурация программных и программно-технических средств, используемых для приема или передачи информации в сеть «Интернет», должны быть стандартизованы, а процессы их установки, настройки, активизации, эксплуатации и обновления должны регламентироваться, протоколироваться и контролироваться.

Все программы, используемые для доступа к сети «Интернет», могут быть установлены на рабочее место только администраторами управления по информационным технологиям и связи администрации города Урай.

Подключение к сети «Интернет» через Wi-Fi на объектах информатизации органов местного самоуправления города Урай осуществляется только через авторизацию пользователя.

3. Запрещается:

1) передавать информацию, отнесенную к информации для служебного пользования;

2) использование сети «Интернет», нарушающее нормы действующего законодательства, этики и корпоративной культуры, а также авторские и смежные права других лиц;

3) посещение сайтов следующего содержания: сайты знакомств, сайты порнографического и эротического содержания, сайты экстремистского содержания и содержания противоречащего нравственным и этническим нормам общества Российской Федерации, сайтов, содержание которых не связано напрямую с выполнением должностных обязанностей работников органов местного самоуправления города Урай;

4) размещать в сети «Интернет» информацию от имени органов местного самоуправления города Урай без согласования руководителя органа местного самоуправления города Урай;

5) публиковать свой адрес, либо адреса других работников органов местного самоуправления города Урай на общедоступных Интернет-ресурсах (форумы, конференции и иные Интернет-ресурсы);

6) предоставлять иным лицам пароль доступа к сети «Интернет»;

7) размещать web-ресурсы органов местного самоуправления города Урай на технических площадках, расположенных вне территории Российской Федерации.

4. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 3 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок использования электронной почты

1. Назначение и область действия.

Порядок использования электронной почты (далее - Порядок) определяет основные требования по защите информации от угроз, связанных с использованием электронной почты.

Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Основные требования.

Использование сети «Интернет» должно быть санкционировано в соответствии с действующей процедурой предоставления доступа к информационным ресурсам и локально-вычислительной сети органов местного самоуправления города Урай.

Электронные почтовые адреса создаются в почтовом домене администрации города Урай или в почтовом домене органа местного самоуправления города Урай.

Использование электронной почты должно осуществляться только для выполнения работниками органа местного самоуправления города Урай своих должностных обязанностей, исключительно в рамках делового общения.

В целях предотвращения несанкционированного распространения информации ограниченного доступа запрещается использовать электронные адреса с хостингом на серверах yandex.ru, mail.ru, dk.ru, gmail.ru и других для передачи информации ограниченного доступа.

Информация ограниченного доступа и другая защищаемая информация, передаваемая с использованием электронной почты, должна быть защищена от несанкционированного просмотра или модификации.

Факты отправки и приема сообщений электронной почты должны фиксироваться, а сообщения - сохраняться.

Перед отправкой сообщений электронной почты необходимо проверять правильность указания адресов получателей.

Состав, архитектура и конфигурация серверов электронной почты органов местного самоуправления города Урай должны быть стандартизованы, а процессы их установки, настройки, эксплуатации должны регламентироваться, протоколироваться и контролироваться.

3. Запрещается:

1) передавать информацию, отнесенную к информации для служебного пользования;

2) использование электронной почты, нарушающее нормы действующего законодательства, этики и корпоративной культуры, а также авторские и смежные права других лиц или представляющее собой любую форму преследования личности;

3) использовать адреса электронной почты для оформления подписок, без предварительного согласования с администратором информационной безопасности;

4) публиковать свой адрес, либо адреса других работников органов местного самоуправления города Урай на общедоступных Интернет-ресурсах (форумы, конференции и иные Интернет-ресурсы);

5) отправлять сообщения с вложенными файлами, общий объем которых превышает 10 Мегабайт;

6) осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как спам и являются незаконными;

7) осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с администратором информационной безопасности;

8) предоставлять иным лицам пароль доступа к своему почтовому ящику;

9) открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

4. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 4 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок организации антивирусной защиты

1. Назначение и область действия.

Порядок организации антивирусной защиты (далее - Порядок) определяет основные требования по защите информационных систем органов местного самоуправления города Урай, связанных с воздействием программ, специально разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации либо копирования информации, а также нарушения нормального функционирования элементов информационно-технологической инфраструктуры.

Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Основные требования.

Установка и настройка средств антивирусной защиты от вредоносных программ (далее – средства защиты) осуществляется администратором информационной безопасности органа местного самоуправления города Урай или специально назначенным лицом в соответствии с эксплуатационной документацией.

Эксплуатация средств защиты должна осуществляться только на основании лицензионных соглашений с их правообладателями. Средства защиты должны иметь все последние обновления, полученные из доверенных источников.

При загрузке автоматизированных рабочих мест (далее - АРМ) в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Установка, конфигурирование, управление средствами антивирусной защиты проводится исключительно администратором информационной безопасности.

Администратор информационной безопасности еженедельно осуществляет проверку статистики обновлений вирусных баз, обновляет базу вручную в случае необходимости.

Полному антивирусному контролю АРМ должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и иных носителях). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения администратором информационной безопасности должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (в том числе, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках) работник самостоятельно или вместе с администратором информационной безопасности должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

1) приостановить работу АРМ;

2) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя органа (структурного подразделения) и администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

3) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4) провести лечение или уничтожение зараженных файлов.

3. Запрещается:

1) использовать внешние носители без предварительной проверки на вредоносные программы;

2) самостоятельно и без согласования с администратором информационной безопасности органа местного самоуправления города Урай устанавливать на АРМ программные продукты для проверки вредоносных программ;

3) игнорировать системные сообщения о выявленных системой вредоносных программах;

4) несанкционированно отключать установленные на АРМ средства для проверки вредоносных программ.

4. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 5 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок проведения технического обслуживания

1. Назначение и область действия.

Порядок проведения технического обслуживания (далее - Порядок) определяет основные требования по обеспечению информационной безопасности при проведении технического обслуживания средств вычислительной техники (СВТ), используемых работниками органов местного самоуправления города Урай.

Порядок распространяется на всех работников органов местного самоуправления города Урай, а так же третьих лиц, выполняющих работы по техническому обслуживанию СВТ органов местного самоуправления города Урай на основании заключенных договоров на обслуживание.

2. Основные требования.

Техническое обслуживание должно осуществляться на основании:

1) обращения пользователя в управление по информационным технологиям и связи администрации города Урай;

2) утвержденных графиков проведения работ по техническому обслуживанию;

3) договоров, муниципальных контрактов.

Все обращения пользователей должны фиксироваться в системе учета заявок администрации города Урай.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест администраторов управления по информационным технологиям и связи администрации города Урай (далее – администратор), конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и должен контролироваться.

Дистанционное техническое обслуживание автоматизированных рабочих мест, на которых используются информационные системы, обрабатывающие информацию ограниченного доступа, разрешено только по защищенному криптографическими средствами каналу связи.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимый для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование информации ограниченного доступа и временное изъятие носителей с такой информацией (в том числе в составе рабочей станции) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих информацию ограниченного доступа, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Администратор, выполняющий техническое обслуживание, вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, несанкционированно установленного или настроенного пользователем.

Передача оборудования для технического обслуживания третьим лицам должна быть согласована с пользователем и управлением по информационным технологиям и связи администрации города Урай и документально оформлена.

3. Запрещается:

1) самостоятельно устанавливать на рабочие места любые дополнительные программные и аппаратные компоненты и устройства;

2) вносить изменения в конфигурацию и настройку рабочих станций;

3) передавать оборудование для технического обслуживания третьим лицам без согласования с управлением по информационным технологиям и связи администрации города Урай.

4. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 6 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок управления доступом к объектам информатизации

1. Назначение и область действия.

Порядок управления доступом к объектам информатизации (далее - Порядок) определяет основные требования по организации и контролю доступа пользователей к объектам информатизации (далее – ОИ) органов местного самоуправления города Урай.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены.

Информационные ресурсы – отдельные документы и массивы документов в информационных системах.

Информационные системы – совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (далее - ИС).

Пользователь – работник органа местного самоуправления города Урай, обрабатывающий информацию в ИС.

Администратор – работник управления по информационным технологиям и связи администрации города Урай, выполняющий функции по администрированию ОИ локально-вычислительной сети администрации города Урай.

Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Основные требования.

Каждый ОИ должен быть закреплен за работником соответствующего органа местного самоуправления города Урай – владельца, в обязанности которого входит определение и пересмотр правил управления доступом и контроль их соблюдения (далее – владелец).

Предоставление доступа к ОИ осуществляется по решению его владельца, согласно определенной владельцем и согласованной с управлением по информационным технологиям и связи администрации города Урай процедуре предоставления доступа в форме заявки, установленной приложением к данному Порядку.

Доступ к ОИ предоставляет администратор данного ИР.

Доступ к ОИ должен предоставляться после проведения оценки связанных рисков, согласно требованиям информационной безопасности и функциональным обязанностям пользователей.

Использование доступа к ОИ должно контролироваться и протоколироваться, а пользователи должны быть осведомлены об ответственности за их неправомерное использование и соблюдать требования по информационной безопасности.

Права доступа пользователей должны регулярно пересматриваться владельцами ОИ на предмет выявления просроченных или избыточных прав, а доступ уволившимся и третьим лицам, завершивших работу, должен быть пересмотрен или удален.

При увольнении непосредственный руководитель пользователя обязан оформить заявку на отключение от всех доступных ему ИР.

Автоматизированные системы управления доступом должны содержать механизмы управления учетными записями и функционировать на основе стандартной процедуры

авторизации пользователей, использующей его учетную запись и уникальный идентификатор (пароль).

Учетная запись пользователя (логин) и пароль передается администратором ИР пользователю способом, исключающим доступ к нему других лиц.

Доступ к ОИ с использованием гостевой учетной записи запрещен, а использование учетных записей с правами администратора и доступ к системным утилитам и средствам диагностики должны подвергаться особому контролю со стороны администратора ИР.

ИР должны быть защищены с использованием межсетевых экранов, а подключение программно-технических средств, обрабатывающих строго конфиденциальную информацию, к телекоммуникационным сетям запрещается.

При использовании удаленного или беспроводного доступа должны использоваться механизмы усиленной аутентификации, шифрования и проверки конфигурации удаленного рабочего места на соответствие требованиям безопасности.

3. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к
Порядку управления
доступом
к объектам
информатизации

Начальнику управления по
информационным технологиям и
связи администрации города Урай
С.А. Осиповой

№

от _____ 20__

ЗАПРОС
о предоставлении (закрытии) доступа

Прошу **предоставить доступ** ☐ /

закрыть доступ ☐ (выбрать нужное)

_____

_____

(обоснование)

к информационному ресурсу _____

_____

Ф.И.О.(ПОЛНОСТЬЮ) и должность пользователя, местонахождение рабочего места и контактный телефон, инвентарный номер ПК	**Полномочия доступа к информационному ресурсу, особые условия доступа (заполняется специалистами отдела по защите информации)**
1	
2	

_____

Руководитель _____ / _____ /

Подпись Расшифровка подписи

Приложение 7 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок физического доступа на объекты информатизации

1. Назначение и область действия.

Порядок физического доступа на объекты информатизации (далее - Порядок) определяет основные требования по защите конфиденциальности информации от угроз, связанных с физическим воздействием на них со стороны человека или факторов внешней среды, в том числе техногенного характера.

Порядок распространяется на всех работников органов местного самоуправления города Урай и третьих лиц, имеющих доступ в помещения органов местного самоуправления города Урай, и является обязательным для исполнения.

2. Основные положения.

Лица, находящиеся в помещениях органов местного самоуправления города Урай, должны соблюдать основные правила пребывания в помещениях и реагирования на чрезвычайные ситуации.

Перемещения оборудования органов местного самоуправления города Урай должны происходить под контролем материально ответственных работников органов местного самоуправления города Урай.

Критичные информационные системы должны размещаться в помещениях с усиленным режимом, оборудованных системами обеспечения и контроля параметров рабочей среды, а списки доступа в помещения должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай и периодически пересматриваться.

Пребывание третьих лиц, а также работников, у которых отсутствует соответствующее разрешение, в местах размещения критичных информационных систем запрещено.

Местонахождение помещений, в которых размещаются критичные информационные системы, не должно отражаться в общедоступных справочниках и указателях.

Телекоммуникационные и силовые кабели критичных информационных систем должны размещаться раздельно в закрытых коробах.

Носители резервных копий должны храниться в отдельных помещениях от резервируемых систем и защищаться от несанкционированного доступа.

Перед передачей оборудования в ремонт или прекращением его использования конфиденциальная информация должна быть удалена. В случае, если неисправность носителя не позволяет удалить конфиденциальную информацию, он должен быть физически уничтожен.

Третьи лица могут находиться в помещениях, где расположены информационные системы, только в сопровождении работников управления по информационным технологиям и связи администрации города Урай.

Мониторы компьютеров должны быть расположены так, чтобы их не было видно из окон зданий, во избежание получения информации с мониторов посторонними лицами.

3. Роли и ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 8 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок инвентаризации информационных активов

1. Назначение и область действия.

1.1. Порядок инвентаризации информационных активов (далее - Порядок) определяет общие положения по инвентаризации информационных активов органов местного самоуправления города Урай, определяет порядок ведения учета информационных активов, правила формирования реестра информационных активов, порядок сбора, анализа, пересмотра и контроля учетной информации об информационных активах.

1.2. В рамках данного Порядка к информационным активам относятся – информационные ресурсы, программное обеспечение, вычислительная техника, технические средства и системы локально-вычислительной сети.

1.3. Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Общие положения.

2.1. Основными целями инвентаризации информационных активов (далее - ИА) являются:

1) ведение учета ресурсов и обеспечение уверенности в их защищенности;

2) идентификация работника соответствующего органа местного самоуправления города Урай - владельца, в обязанности которого входит определение и пересмотр правил управления доступом и контроль их соблюдения, ответственность за обработку данных (далее – владелец) и определение его ответственности за поддержание соответствующих мероприятий по управлению информационной безопасности;

3) идентификация относительной ценности и важности ресурсов для управления рисками;

4) сбор информации для планирования бюджетных расходов на создание, модернизацию, приобретение и эксплуатацию ИА.

Инвентаризация ИА проводится сотрудниками управления по информационным технологиям и связи администрации города Урай.

2.2. Периодичность инвентаризации:

1) планово один раз в год;

2) при вводе в эксплуатацию ИА;

3) при изменении состава ИА (установка программного обеспечения, замена оборудования).

2.3. По результатам инвентаризации:

1) на каждое рабочее место оформляется паспорт рабочего места. Паспорт рабочего места оформляется в двух экземплярах, один экземпляр находится у пользователя рабочего места или владельца ИА, второй экземпляр в управлении по информационным технологиям и связи администрации города Урай;

2) формируется сводный перечень информационных систем органов местного самоуправления города Урай.

2.4. Все информационные активы учитываются в базе данных с помощью программного обеспечения «HARDWARE INSPECTOR».

Информационные системы органов местного самоуправления города Урай учитываются в едином реестре информационных систем Ханты-Мансийского

автономного округа – Югры на основании постановления Правительства Ханты-Мансийского автономного округа - Югры от 18.01.2008 № 6-п «О Едином реестре информационных систем Ханты-Мансийского автономного округа – Югры».

3. Роли и ответственность.

3.1. Ответственность за проведение инвентаризации ИА, достоверность сведений, поддержку актуального состояния базы данных «HARDWARE INSPECTOR», регистрацию ИС в едином реестре информационных систем Ханты-Мансийского автономного округа – Югры несет управление по информационным технологиям и связи администрации города Урай.

3.2. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 9 к
постановлению
администрации города
Урай
от 26.09.2022 № 968

Инструкция по организации резервного копирования (восстановления) данных, обрабатываемых в информационных системах

1. Назначение и область действия.

1.1. Инструкция по организации резервного копирования (восстановления) данных, обрабатываемых в информационных системах (далее - Инструкция), определяет основные требования и объемы резервирования данных, хранящихся в информационных системах (далее – ИС) органов местного самоуправления города Урай, а также порядок восстановления работоспособности информационных систем.

1.2. Порядок распространяется на всех работников органов местного самоуправления города Урай, осуществляющих администрирование ИС (далее – администраторов), и является обязательной для исполнения.

2. Общие положения.

2.1. Настоящая инструкция определяет:

1) порядок резервированного копирования данных для последующего восстановления работоспособности ИС при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и другими обстоятельствами);

2) порядок восстановления данных в случае возникновения такой необходимости;

3) требования к работе пользователей и администраторов ИС, связанных с резервным копированием и восстановлением данных.

2.2. Резервному копированию подлежит информация следующих основных категорий:

1) персональная информация пользователей (личные каталоги на файловых серверах);

2) групповая информация пользователей (общие каталоги отделов);

3) информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);

4) информация ИС, в том числе баз данных;

5) рабочие копии установочных компонентов программного обеспечения ИС;

6) программное обеспечение средств защиты информации.

3. Порядок резервного копирования.

3.1. Резервное копирование данных, обрабатываемых в ИС, производится на основании состава и объема копируемых данных, периодичности проведения резервного копирования в соответствии с перечнем информации, подлежащей резервному копированию, форма которого установлена приложением к Инструкции.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

3.2. Методика проведения резервного копирования:

Для организации системы резервного копирования используется специализированное программное обеспечение (далее - ПО).

С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в ночное время.

3.3. Для резервирования информации используются следующие виды резервного копирования:

1) Полное резервирование Full Backup:
2) Дифференциальное резервирование Differential Backup;
3) Добавочное резервирование Incremental Backup.

По запросу владельца ИР может производиться одноразовое полное копирование информации.

3.4. Для резервирования информации используются следующие наборы резервных копий:

1) Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – год.
2) Недельная копия. Записывается в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы.
3) Ежедневная копия. Записывается ежесуточно, кроме ночи на субботу. Срок хранения – неделя.

3.5. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервных копий осуществляется на жёсткий диск. Два жёстких диска на сервере дублируют друг друга.

Для резервирования информации, хранимой в базах данных прикладной информационной системы, в качестве промежуточного звена автоматизации используются средства конфигурирования прикладной информационной системы и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных прикладной ИС. Посредством ПО формируются задания на проведение резервного копирования этого каталога. При этом настраивается срок хранения информации и периодичность выполнения резервного копирования.

4. Требования к внешним носителям информации.

4.1. Учитывая пропускные способности каналов, стоимость трафика между офисами, объёмы резервируемых данных, требования программного обеспечения ИС, требования защиты информации, для резервного копирования данных ИС и их хранения могут использоваться внешние носители информации.

4.2. Все внешние магнитные, оптические и другие машинные носители, используемые для хранения резервных копий, подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет.

4.3. Внешние носители должны храниться в безопасных, надежных условиях с учетом требований по информационной безопасности.

4.4. Уничтожение информации с магнитных носителей информации должно осуществляться средствами гарантированного уничтожения информации.

5. Контроль результатов резервного копирования.

5.1. Контроль результатов всех процедур резервного копирования осуществляется администратором в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

5.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

6. Восстановление информации из резервных копий.

6.1. Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанного с потерей работоспособности ИС или ее компонента, выполняется на основании заявки, оформленной через систему обработки заявок администрации города Урай.

Восстановление информации, относящейся к базам ИС, происходит при тесном взаимодействии владельца информации с администратором ИС.

6.2. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования программного обеспечения.

6.3. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

7. Роли и ответственность.

7.1. Ответственность за соблюдение указанных требований возлагается на всех администраторов и владельцев информационных ресурсов органов местного самоуправления города Урай, ответственных за резервное копирование данных ИС.

7.2. Ответственность за ведение перечня информации, подлежащей резервному копированию, администрирование программного обеспечения резервного копирования возлагается на управление по информационным технологиям и связи администрации города Урай.

7.3. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к Инструкции
по организации резервного
копирования
(восстановления) данных,
обрабатываемых в
информационных системах

Перечень информации, подлежащей резервному копированию.

№	Наименование информационного ресурса	Место размещения информационного ресурса	Вид резервного копирования (период возобновляемого копирования)	Место хранения копии	Ответственное лицо

Приложение 10 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок управления инцидентами по информационной безопасности

1. Назначение и область действия.

1.1. Порядок управления инцидентами по информационной безопасности (далее - Порядок) определяет основные требования к обработке инцидентов информационной безопасности.

1.2. К инцидентам информационной безопасности (далее – ИБ) могут относиться: несанкционированное использование информационных ресурсов и систем, их нетипичное функционирование, опасность физического повреждения или уничтожения, наличие уязвимостей, нарушения требований нормативных документов по информационной безопасности, иные происшествия, так или иначе связанные с информационной безопасностью.

1.3. Порядок распространяется на всех работников органов местного самоуправления города Урай и является обязательным для исполнения.

2. Основные требования.

2.1. Извещение об инцидентах ИБ.

При обнаружении явного или предполагаемого инцидента ИБ следует максимально зафиксировать его характерные признаки и сопутствующие ему обстоятельства и немедленно поставить в известность администратора информационной безопасности управления по информационным технологиям и связи администрации города Урай (далее – администратора информационной безопасности) посредством телефона, факса, электронной почты, личного обращения, либо в системе обработки заявок администрации города Урай.

2.2. Реагирование и обработка инцидентов ИБ.

Все поступающие сообщения об инцидентах ИБ должны регистрироваться в системе обработки заявок администрации города Урай со статусом «Инцидент по ИБ» и фиксироваться в журнале учета инцидентов ИБ, форма которого установлена приложением к Порядку.

Обработка инцидентов ИБ осуществляется администратором информационной безопасности. При необходимости к обработке инцидента ИБ привлекается владелец информационного ресурса, затронутого инцидентом.

Обработка инцидентов должна осуществляться в следующем порядке:

1) сбор и фиксация информации об инциденте с целью установления его причины и обеспечения доказательственной базы для расследования;

2) выработка, доведение до исполнителей и координация выполнения плана экстренных действий по локализации и пресечению негативного воздействия, минимизации ущерба и восстановлению нарушенных бизнес-процессов;

3) выработка, доведение до исполнителей и координация выполнения плана работ по устранению уязвимости для недопущения повторения инцидента;

4) оценка ущерба и, при необходимости, проведение служебного расследования с представлением отчёта руководству.

2.3. Заключения о результатах обработки инцидента ИБ заносятся в систему обработки заявок администрации города Урай.

2.4. Результаты накопления, обобщения и анализа инцидентов могут служить основанием для внесения изменений в организационно-распорядительные акты по информационной безопасности.

3. Роли и ответственность.

3.1. Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

3.2. Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами, является грубым нарушением трудовой дисциплины.

3.3. Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

3.4. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к Порядку управления инцидентами по информационной безопасности

ЖУРНАЛ

учета инцидентов информационной безопасности

№ № п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

Приложение 11 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Порядок работы с криптосредствами и электронной подписью

1. Назначение и область действия.

1.1. Порядок работы с криптосредствами и электронной подписью (далее - Порядок) регламентирует порядок обращения со средствами криптографической защиты информации (далее - СКЗИ) и электронной подписью (далее ЭП), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

1.2. Все работники органов местного самоуправления города Урай, допущенные к работе с СКЗИ и ЭП, должны ознакомиться с данным порядком под подпись и строго выполнять установленные требования настоящего Порядка в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

2. Основные требования.

2.1. Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ и ЭП осуществляется ответственным за эксплуатацию СКЗИ и ЭП.

2.2. Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц.

2.3. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

2.4. Пользователю СКЗИ и ЭП не допускается:

1) разглашать информацию о ключевых документах;

2) допускать вывод ключевых документов на монитор компьютера или принтер;

3) допускать установки ключевых документов в другие компьютеры;

4) записывать на внешний носитель с ключами, информации постороннего содержания;

5) изменять программное обеспечение СКЗИ и средств ЭП;

6) сохранять новые ключи на внешнем носителе без форматирования старых;

7) использовать вредоносные программы (в том числе вирусы) на компьютере с установленными СКЗИ и средствами ЭП.

2.5. Пользователь должен соблюдать правила пользования СКЗ и ЭП:

1) можно использовать только в системе передачи данных по телекоммуникационным каналам связи;

2) можно использовать для шифрования конфиденциальной информации, не содержащей государственной тайны;

3) СКЗИ и ЭП действуют в течение одного года с момента их создания, а по истечению должны быть заменены.

2.6. Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный

учет в журнале, форма которого установлена приложением к Порядку. Ведет журналы администратор информационной безопасности.

2.7. Единицей поэкземплярного учета СКЗИ является:

1) для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

2) для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и иные носители).

2.8. Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

2.9. Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

2.10. В случае отсутствия у сотрудника индивидуального хранилища, инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за эксплуатацию СКЗИ и ЭП.

2.11. В случае утери носителя СКЗИ и ЭП или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за эксплуатацию СКЗИ и ЭП.

2.12. Ответственным за эксплуатацию СКЗИ и ЭП периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

3. Действия пользователя по восстановлению связи в случае компрометации действующих ключей к СКЗИ.

3.1. Под компрометацией ключей подразумевается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

3.2. Основные события, квалифицируемые как компрометация ключей:

1) посторонним лицам мог стать доступным файл ключевого дистрибутива;

2) посторонним лицам мог стать доступным съемный носитель с ключевой информацией;

3) посторонним лицам мог стать доступным пароль пользователя, и эти лица могли иметь доступ к компьютеру пользователя;

4) посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;

5) увольнение сотрудников, имевших доступ к ключевой информации;

6) нарушение печати на сейфе с ключевыми носителями;

7) наличие в подписи под входящим документом сертификата, находящегося в списке отозванных сертификатов;

8) случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

3.3. К событиям, требующим расследования и принятия решения по компрометации, относятся возникновение подозрений по утечке или искажению информации в системе конфиденциальной связи.

3.4. При наступлении любого из перечисленных событий пользователь должен немедленно прекратить работу на своем автоматизированном рабочем месте и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору информационной безопасности.

Возобновление работы на своем автоматизированном рабочем месте пользователю разрешается только после получения уведомления о возможности работы от администратора информационной безопасности.

4. Роли и ответственность.

4.1. Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

4.2. Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

4.3. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к Порядку
работы с криптосредствами и
электронной подписью

Журнал учета СКЗИ и ЭП

(лист 1)

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

(лист 2)

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
ФИО. пользователя криптосредств, производившего подключение (установку)	дата подключения (установки) и подписи лиц, произведших подключение (установку)	номера аппаратных средств, в которые установлены или к которым подключены криптосредства	дата изъятия (уничтожения)	ФИО. пользователя СКЗИ, производившего изъятие (уничтожение)	номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 12 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Инструкция пользователя
по работе с объектами информатизации

1. Общие положения.

Настоящая Инструкция пользователя по работе на объектах информатизации (далее –Инструкция) определяет основные положения и требования по обеспечению информационной безопасности (далее - ИБ) на рабочих местах всех работников органов местного самоуправления города Урай (далее – пользователь) и регулирует порядок работы с информационными ресурсами (далее - ИР) в локально-вычислительной сети (далее - ЛВС) администрации города Урай.

Инструкция является документом, обязательным для исполнения всеми пользователями ЛВС администрации города Урай.

2. Основные требования.

Пользователь обязан строго соблюдать установленные правила работы на объектах информатизации и несет персональную ответственность за неукоснительное выполнение требований и мероприятий по защите информации на своих автоматизированных рабочих местах (далее – АРМ).

Пользователь обязан:

1) знать и выполнять требования нормативных правовых документов по обеспечению информационной безопасности Российской Федерации;

2) руководствоваться требованиями следующих утвержденных постановлением администрации города Урай документов: Порядок использования паролей, Порядок использования сети «Интернет», Порядок использования электронной почты, Порядок антивирусной защиты, Порядок проведения технического обслуживания, Порядок управления доступом к объектам информатизации, Порядок физического доступа на объекты информатизации, Порядок инвентаризации информационных систем, Инструкция по организации резервного копирования (восстановления) данных, обрабатываемых в информационных системах, Порядок управления инцидентами по информационной безопасности, Порядок работы с криптосредствами и электронной подписью;

3) получить уникальный идентификатор (имя учетной записи) и пароль после прохождения согласования заявки на предоставление доступа в соответствии с его должностными обязанностями;

4) располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления посторонними лицами с отображаемой на нем информацией;

5) при выходе из помещения в течение рабочего дня выключать или блокировать АРМ;

6) после завершения работы производить блокировку или выключение АРМ;

7) соблюдать правила работы со средствами защиты информации (далее – СЗИ) и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с конфиденциальной информацией при ее обработке;

8) уметь пользоваться средствами антивирусной защиты и при необходимости проверять АРМ на наличие вредоносных программ (вирусов);

9) при необходимости изменения прав доступа проинформировать своего руководителя о необходимости таких изменений;

10) помнить личные пароли и идентификаторы;

11) докладывать администратору информационной безопасности о фактах компрометации пароля, несанкционированного доступа со стороны других пользователей, случаях утечки и нарушения целостности информации, обрабатываемой в ИР, нарушениях целостности компонентов системы защиты информации.

3. Пользователю запрещается:

1) использовать АРМ в неслужебных целях;

2) самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами на АРМ (техническим паспортом);

3) осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

4) осуществлять обработку конфиденциальной информации при неисправных СЗИ;

5) записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (бумажных носителях, гибких магнитных дисках и т.п.);

6) оставлять включенной без присмотра на короткое или длительное время АРМ, не активировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

7) делать неучтенные копии личных идентификаторов, ключевой дискеты, карточки пароля (и других реквизитов доступа);

8) снимать защиту от записи с машинного носителя информации, вносить какие-либо изменения в файлы ключевой дискеты и личных идентификаторов;

9) использовать личные идентификаторы и свой носитель для формирования цифровой подписи любых электронных документов, кроме как предусмотренных технологическим процессом на рабочем месте.

4. Пользователь имеет право:

1) обращаться за помощью к специалистам управления по информационным технологиям и связи администрации города Урай при решении задач использования ИР ЛВС администрации города Урай.

2) При возникновении технической или программной проблемы на рабочем месте, пользователь должен сделать заявку по телефону 29500 (внутренний номер 300) либо в системе обработки заявок администрации города Урай по адресу: http://portal/HWISD/default.aspx.

3) обращаться к администратору безопасности информации с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой в АС информации, а также по вопросам эксплуатации установленных СЗИ;

4) вносить предложения по улучшению работы с ИР и ЛВС администрации города Урай.

5. Ответственность.

Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение 13 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Инструкция по работе с машинными носителями информации в информационных системах

1. Общие положения.

1.1. Настоящая Инструкция по работе с машинными носителями информации в информационных системах (далее – Инструкция) регламентирует порядок использования и работы со съемными носителями информации во всех информационных системах органов местного самоуправления города Урай, подлежащих защите в соответствии с требованиями законодательства.

1.2. Инструкция является документом, обязательным для исполнения всеми пользователями информационных систем (далее – ИС) органов администрации города Урай.

2. Порядок использования съемных носителей информации.

2.1. Под использованием съемных носителей информации в ИС понимается их подключение к автоматизированным рабочим местам (далее – АРМ) с целью обработки, приема/передачи информации между АРМ и носителями информации.

2.2. В ИС допускается использование только учтенных съемных носителей информации, которые являются собственностью органа администрации города Урай (далее – Учреждения) и подвергаются регулярной ревизии и контролю.

2.3. Съемные носители информации предоставляются пользователям ИС по инициативе руководителей органов (структурных подразделений) в случаях:

1) необходимости выполнения вновь принятым работником своих должностных обязанностей;

2) возникновения у сотрудника Учреждения производственной необходимости.

3. Порядок учета, хранения и обращения со съемными носителями, твердыми копиями и их утилизации.

3.1. Все находящиеся на хранении и в обращении съемные носители подлежат учёту.

3.2. Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Для получения электронного внешнего носителя, пользователь обращается к непосредственному руководителю, который пишет служебную записку на имя ответственного за организацию работ по защите персональных данных и другой защищаемой информации в Учреждении о выдаче пользователю внешнего электронного носителя. Ответственный за организацию работ по защите информации принимает решение и передает служебную записку администратору информационной безопасности.

3.4. Учет и выдачу съемных носителей осуществляет администратор информационной безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета машинных носителей конфиденциальной информации, форма которого установлена согласно приложению к Инструкции.

3.5. При использовании пользователями съемных носителей информации необходимо:

1) соблюдать требования настоящей Инструкции;

2) использовать носители информации исключительно для выполнения своих служебных обязанностей;

3) ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;

4) бережно относится к носителям информации;

5) извещать администратора информационной безопасности о фактах утраты (кражи) носителей информации.

3.6. При использовании носителей конфиденциальной информации запрещено:

1) использовать носители конфиденциальной информации в личных целях;

2) передавать носители конфиденциальной информации другим лицам (за исключением администратора информационной безопасности);

3) хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

4) выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны (в том числе для работы с ними на дому).

3.7. Любое взаимодействие (обработка, прием/передача информации), инициированное пользователем ИС между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором информационной безопасности). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

3.8. Факт несанкционированного и/или нецелевого использовании носителей информации считается инцидентом информационной безопасности. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю органа (структурного подразделения) для принятия мер согласно утвержденному постановлением администрации города Урай Порядку управления инцидентами по информационной безопасности.

3.9. Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.10. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего органа (структурного подразделения). На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

3.11. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

3.12. В случае увольнения или перевода работника в другой орган (структурное подразделение) предоставленные носители конфиденциальной информации сдаются администратору информационной безопасности.

4. Роли и ответственность.

4.1. Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

4.2. Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай,

несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

4.3. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к Инструкции по работе с машинными носителями информации в информационных системах

ЖУРНАЛ
учета машинных носителей конфиденциальной информации

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

Приложение 14 к
постановлению
администрации города Урай
от 26.04.2022 № 968

Инструкция по использованию программных и аппаратных средств защиты информации

1. Общие положения.

1.1. Настоящая Инструкция по использованию программных и аппаратных средств защиты информации (далее – Инструкция) определяет порядок эксплуатации средств защиты информации (далее - СЗИ) во всех подлежащих в соответствии с требованиями законодательства защите информационных системах органов администрации города Урай.

1.2. Инструкция является документом, обязательным для исполнения всеми пользователями информационных систем (далее – ИС) и администратором информационной безопасности органов администрации города Урай.

2. Порядок эксплуатации средств защиты информации.

2.1. Для обеспечения необходимого уровня защищенности при работе в ИС органов администрации города Урай применяются следующие средства защиты информации:

1) Средство антивирусной защиты информации «Антивирус Касперского».
2) Средство защиты информации от несанкционированного доступа «Secret Net».
3) Персональный межсетевой экран и клиент защищенной почтовой системы «ViPNet Client X.X».
4) Подсистема анализа защищенности Сканер –ВС.
5) Подсистема защиты среды виртуализации vGate R2.
6) Подсистема обнаружения вторжений ПАК VipNet IDS 100.
7) Подсистема криптографической защиты ПАК VipNet Coordinator.

2.2. Эксплуатация СЗИ осуществляется в соответствии с эксплуатационной документацией, предоставляемой производителями средств защиты информации.

Пользователи должны быть ознакомлены с инструкциями по работе со СЗИ в части их касающейся.

Контроль по выполнению пользователями требований документов по эксплуатации СЗИ возлагается на администратора информационной безопасности.

2.3. Порядок установки, настройки, модификации и технического обслуживания СЗИ.

В соответствии с Федеральным законом от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности» и постановлением Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации» выполнение работ по установке, монтажу, испытаниям, ремонту средств защиты информации отнесены к лицензируемому виду деятельности по технической защите конфиденциальной информации. Для выполнения указанных работ может привлекаться только организация, имеющая соответствующую лицензию.

2.4. Эксплуатация средств защиты информации осуществляется лицами, допущенными к ним в соответствии с Разрешительной системой доступа персонала к сведениям конфиденциального характера в ИС.

2.5. Внесение изменений в конфигурацию используемых СЗИ осуществляет администратор безопасности информации.

2.6. Эксплуатируемые СЗИ защиты учитываются администратором информационной безопасности в Журнале учёта средств защиты информации, форма которого установлена приложением к Инструкции.

3. Роли и ответственность.

3.1. Ответственность за соблюдение указанных требований возлагается на всех работников органов местного самоуправления города Урай.

3.2. Все исключения из основных требований должны быть согласованы с управлением по информационным технологиям и связи администрации города Урай, несогласованные отступления расцениваются в качестве инцидентов информационной безопасности и могут служить основанием для привлечения к ответственности, предусмотренной федеральным законодательством.

3.3. Контроль за выполнением указанных требований и их пересмотр возлагаются на управление по информационным технологиям и связи администрации города Урай.

Приложение к Инструкции
по использованию
программных и аппаратных
средств защиты информации

Журнал
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечани