Муниципальное
бюджетное учреждение
культуры
**«Творческо-методический
центр»**
Оренбургского района
Оренбургской области
Почтовый адрес: 460527,
Оренбургская обл., Оренбургский р-
он, п. Караванный, ул. Советская, д 8
тел/факс 535951
e-mail: orentmz@mail.ru

ПРИКАЗ

«04» октября 2024 № 45

«О защите персональных данных»

В целях повышения уровня обеспечения информационной безопасности, информационно-телекоммуникационной инфраструктуры, в соответствии с Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также во исполнение требований, установленных гл. 14 Трудового кодекса Российской Федерации, а также Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Положение об организации парольной защиты Муниципального бюджетного учреждения культуры «Творческо-методический центр» Оренбургского района Оренбургской области и ввести его в действие с 01.10.2024 г. (Приложение № 1).
2. Утвердить Положение об организации антивирусной защиты в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области и ввести его в действие с 01.10.2024 г. (Приложение № 2).
3. Утвердить Положение об использовании сети Интернет в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области и ввести его в действие с 01.10.2024 г. (Приложение № 3).
4. Контроль за исполнением приказа оставляю за собой.

Руководитель О.В. Моисеева

С приказом ознакомлен (а) _____

Приложение № 1
к Приказу № 45
от «04» октября 2024 г.

Положение
об организации парольной защиты в
Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области

1. Общие положения

1.1. Положение об организации парольной защиты в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области (далее – Положение) регламентирует:

организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной среде;

меры обеспечения безопасности при использовании паролей;

меры контроля за действиями пользователей и обслуживающего персонала при работе с паролями.

1.2. Требования настоящего Положения:

являются неотъемлемой частью комплекса мер безопасности и защиты информации в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области (далее – МБУК ТМЦ Оренбургского района);

распространяются на сотрудников МБУК ТМЦ Оренбургского района;

обязательны к применению для всех средств вычислительной техники, эксплуатируемой в МБУК ТМЦ Оренбургского района, а также информационных систем и сервисов, используемых сотрудниками МБУК ТМЦ Оренбургского района.

1.3. Ознакомление с Положением является выражением согласия с персональной ответственностью за разглашение парольной информации лицам, не имеющим права на доступ к таким сведениям.

1.4. Сведения о логине и пароле в сочетании и раздельно – являются конфиденциальной информацией, на которую распространяется действие нормативных правовых актов МБУК ТМЦ Оренбургского района, принятых в отношении конфиденциальной информации.

1.5. Термины и определения:

Автоматизированная система (АС) – совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки информации и производства вычислений.

АРМ (автоматизированное рабочее место) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида АС.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности работы и минимизации рисков.

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск, токен и т.п.), на котором находится ключевая информация (ключи доступа, пароли, любая информация, позволяющая получить привилегии, права, полномочия в информационной среде).

Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

Несанкционированный доступ (НСД) – доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Принцип минимальных привилегий – принцип, согласно которому каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в результате случайного, ошибочного или несанкционированного использования системы.

Сотрудник – муниципальный служащий, замещающий должность муниципальный службы в МБУК ТМЦ Оренбургского района.

- Учетная запись – информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и право выполнения определенных операций с данными в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

2. Общие требования к паролям

2.1. Пароли доступа к информационной системе (сервису) первоначально формируются оператором данной системы (сервиса) или назначенным на данную роль сотрудником. В дальнейшем пользователь информационной системы (сервиса) должен самостоятельно изменить пароль на собственный, с учетом требований Положения, предъявляемых к паролю.

2.2. Запрещается использовать в качестве пароля любую информацию, относящуюся к сотруднику или месту его работы (дата или год рождения сотрудника или близких ему людей, имена детей, клички домашних животных и др.).

2.3. Пароли должны отвечать следующим требованиям:

- длина пароля должна быть не менее 10 символов (для привилегированных учетных записей – не менее 12 символов);

- при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами.

3. Безопасность локальных учетных записей на АРМ работников

3.1. Локальные учетные записи на АРМ сотрудников используются только при настройке операционной системы и не предназначены для повседневной работы.

3.2. Пользователям запрещено создание и использование учетных записей на АРМ, подключенных к компьютерной сети МБУК ТМЦ Оренбургского района и входящих в состав домена либо какого-либо из его поддоменов.

3.3. Встроенная гостевая учетная запись должна быть заблокирована на всех АРМ в составе компьютерной сети МБУК ТМЦ Оренбургского района при первоначальном конфигурировании операционной системы.

3.4. Встроенная административная учетная запись операционной системы на АРМ МБУК ТМЦ Оренбургского района должна быть отключена администратором домена. Допускается отсутствие блокировки административной учетной записи операционной системы, если АРМ МБУК ТМЦ Оренбургского района не включен в домен. В этом случае такая учетная запись должна быть защищена паролем, отвечающим требованиям п. 8 Положения.

3.5. Базовая система ввода-вывода (BIOS) рабочих станций на АРМ МБУК ТМЦ Оренбургского района должна быть защищена паролем длиной не менее 8 символов.

4. Безопасность учетных записей работников МБУК ТМЦ Оренбургского района

4.1. Создание, изменение, удаление учетной записи сотрудника МБУК ТМЦ Оренбургского района (домен, электронная почта и др.) производится после получения заявки от МБУК ТМЦ Оренбургского района, для сотрудника которого необходимо выполнить одно из указанных выше действий.

4.2. Сотрудник несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.

4.3. Допускается раскрытие пароля работника при проведении проверочных мероприятий управлением информационной безопасности МБУК ТМЦ Оренбургского района или при производственных работах. После данных работ работник самостоятельно производит немедленную смену «раскрытых» паролей.

4.4. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имени и пароля сотрудника (в его отсутствие) допускается изменение пароля руководителем сотрудника. В таких случаях, сотрудник, чей пароль был изменен, обязан после выявления факта смены своего пароля, незамедлительно создать новый пароль.

4.5. Пароли учетных записей пользователей АС должны соответствовать требованиям п. 8 Положения.

4.6. Управление доменными учетными записями пользователей осуществляется исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа как к локальной системе, так и к ресурсам АС больше, чем это необходимо ему для выполнения своих должностных обязанностей.

4.7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к сотруднику, обслуживающему контроллер домена, или АС МБУК ТМЦ Оренбургского района.

4.8. Внеплановая смена личного пароля или удаление учетной записи пользователя АС в случае прекращения его полномочий (увольнение, перевод и иные обстоятельства.) должна организовываться МБУК ТМЦ Оренбургского района, в котором он осуществляет трудовую функцию, незамедлительно после окончания последнего сеанса работы данного пользователя.

4.9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу и иные обстоятельства) сотрудников, которым были предоставлены полномочия по управлению парольной защитой подсистем контроллера домена или АС МБУК ТМЦ Оренбургского района.

4.10. В случае длительного (более 14 дней) отсутствия сотрудника МБУК ТМЦ Оренбургского района (командировка, болезнь и т.п.) его учетная запись блокируется.

4.11.В случае компрометации или утраты личного пароля либо подозрения на компрометацию сотрудником МБУК ТМЦ Оренбургского района незамедлительно должны быть предприняты меры по внеплановой смене личного пароля с информированием МБУК ТМЦ Оренбургского района, в котором он осуществляет трудовую функцию.

4.12. В случае, если сотрудник МБУК ТМЦ Оренбургского района забыл личный пароль (и при этом пароль не скомпрометирован и не утрачен) он обязан обратиться к администратору контроллера домена или АС МБУК ТМЦ Оренбургского района с просьбой о восстановлении пароля. Администратор контроллера домена или АС обязан установить временный пароль в соответствие с требованиями п. 8 Положения. Пользователь после получения временного пароля обязан в кратчайшее время (не более 30 минут) сменить временный пароль.

4.13.Для предотвращения подбора паролей в контроллере домена или АС МБУК ТМЦ Оренбургского района должна осуществляться блокировка учетной записи при пятикратном неправильном вводе пароля.

4.14.При временном оставлении рабочего места в течение рабочего дня сотрудник обязан заблокировать АРМ до интерфейса с предложением о входе в операционную систему.

4.15.При возникновении вопросов или проблем, связанных с использованием учетных записей домена или АС сотрудник обязан уведомить МБУК ТМЦ Оренбургского района и обратиться к администратору домена или АС.

5. Временные учетные записи

5.1. Для предоставления временного доступа к ресурсам АС МБУК ТМЦ Оренбургского района используется процедура предоставления временных учетных записей.

5.2. Временная учетная запись – учетная запись, имеющая ограничение по времени действия и ограниченный набор прав использования ресурса. Для временных учетных записей проводится подробное протоколирование их использования. Процедура получения временных учетных:

- сотрудник МБУК ТМЦ Оренбургского района оформляет заявку на предоставление временного доступа к информационным, программным и аппаратным ресурсам МБУК ТМЦ Оренбургского района. В заявке указываются: временной интервал использования временной учетной записи, сведения о лице (ФИО, место работы), которое будет использовать временную учетную запись, права, необходимые для такой учетной записи. Заявка утверждается МБУК ТМЦ Оренбургского района и направляется на согласование.
- после согласования МБУК ТМЦ Оренбургского района, заявка направляется оператору ресурса, к которому необходимо предоставить доступ;
- временная учетная запись создается оператором ресурса, реквизиты учетной записи передаются заявителю с соблюдением установленных в МБУК ТМЦ Оренбургского района требований по безопасности конфиденциальной информации;
- пользователь, получивший временную учетную запись, информируется об ограничениях, связанных с ее использованием;
- при необходимости пользователь может оформить заявку с просьбой продлить срок действия временной учетной записи с кратким объяснением причин такой необходимости.

6. Безопасность привилегированных учетных записей

6.1. К привилегированным учетным записям относятся учетные записи, используемые для управления работой, АС (учетные записи администраторов).

6.2. При использовании привилегированных учетных записей необходимо руководствоваться принципом «минимальных привилегий», т.е.

привилегии администратора должны использоваться только администратором и только если выполняемая задача требует наличия таких привилегий.

6.3. Недопустимо использование привилегированных учетных записей в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление операционной системы, сервисов и т.п.).

6.4. Учетная запись администратора домена может использоваться только при установке, конфигурировании, восстановлении контроллера домена и иных действиях, при которых использование других учетных записей невозможно. Для этой учетной записи проводится подробное протоколирование всех событий ее использования, а также немедленное расследование любого нецелевого ее использования.

6.5. Для служб и сервисов используется принцип «минимальных привилегий», т.е. службы и сервисы функционируют с минимально возможными для их корректной работы привилегиями.

6.6. К учетным записям серверов высокой степени критичности (контроллеры домена, серверы баз данных, иные серверы, от которых зависит бесперебойная работа АС МБУК ТМЦ Оренбургского района) предъявляются повышенные требования к привилегиям удаленного доступа.

6.7. В случае компрометации, либо подозрения на компрометацию привилегированной учетной записи проводится внеплановая смена паролей всех зависящих от нее учетных записей.

7. Аппаратные средства аутентификации

7.1. Для повышения степени защиты критически важных объектов АС МБУК ТМЦ Оренбургского района (рабочие станции и мобильные компьютеры с информацией высокой степени конфиденциальности, иные объекты) от несанкционированного доступа возможно использование двухфакторной аутентификации (по паролю и предмету – далее ключевой носитель информации).

7.2. Каждому пользователю АС МБУК ТМЦ Оренбургского района, для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации, который учитывается управлением информационной безопасности МБУК ТМЦ Оренбургского района установленным образом (однозначное сопоставление ключевого носителя и его владельца).

7.3. Ключевые носители информации маркируются управлением информационной безопасности МБУК ТМЦ Оренбургского района установленным образом (уникальный номер ключевого носителя) или используется серийный номер производителя.

7.4. В случае прекращения необходимости использования персонального ключевого носителя (увольнение сотрудника, прекращение функционирования объекта, для аутентификации на котором носитель использовался и т.п.) информация с данного носителя удаляется

установленным образом, либо уничтожается сам носитель в случае невозможности его очистки.

7.5. Пользователям АС МБУК ТМЦ Оренбургского района категорически запрещается оставлять без личного присмотра ключевые носители, сообщать коды от персонального ключевого носителя, если таковые имеются.

7.6. Передача ключевого носителя пользователем третьему лицу допускается только при оформлении доверенности в письменной форме с указанием допустимых действий с данным носителем (хранение, использование). Доверенность должна содержать сведения, позволяющие определить:

- лиц передающего и получающего ключевой носитель;
- цель передачи/получения ключевого носителя;
- допустимые действия с ключевым носителем, которые получающая сторона может выполнять с ключевым носителем;
- срок, в течении которого получающая сторона в праве совершать указанные действия с ключевым носителем.

7.7. В случае утраты персонального ключевого носителя пользователь (доверенное лицо) обязан немедленно сообщить об инциденте руководителю структурного подразделения МБУК ТМЦ Оренбургского района. При возникновении подобного инцидента необходимо незамедлительно принять меры для недопущения несанкционированного использования утраченного персонального ключевого носителя.

8. Ответственность

8.1. Пользователи АС МБУК ТМЦ Оренбургского района несут персональную ответственность за несоблюдение требований настоящего Положения.

Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам АС МБУК ТМЦ Оренбургского района действиями либо бездействием соответствующего работника.

Приложение № 2
к Приказу № 45
от «04» октября 2024 г.

ПОЛОЖЕНИЕ
об организации антивирусной защиты в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области

1. Общие положения

1.1. Настоящее Положение разработано во исполнение федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», с учетом ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и устанавливает порядок антивирусной защиты и антивирусного контроля в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области (далее – МБУК ТМЦ Оренбургского района).

1.2. Настоящее Положение разработано в целях осуществления антивирусной защиты информационных ресурсов МБУК ТМЦ Оренбургского района.

1.3. Целью мероприятий по антивирусной защите является:

- защита информационных ресурсов МБУК ТМЦ Оренбургского района от несанкционированного копирования, искажения и разрушения;
- минимизация риска отказов и нестабильной работы технологических и информационных процессов, при воздействии вирусов и других вредоносных программ;
- минимизация финансовых, репутационных потерь и трудовых затрат при устранении последствий воздействия вредоносного кода.

1.4. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в МБУК ТМЦ Оренбургского района.

1.5. Требования настоящего Положения распространяются на сотрудников МБУК ТМЦ Оренбургского района и применяются для всех объектов информатизации, эксплуатируемых в МБУК ТМЦ Оренбургского района.

2. Термины, определения, сокращения

Пользователь САВЗ – пользователь ОИ, на котором установлен САВЗ.

САВЗ – средство антивирусной защиты.

ОИ – объект информатизации. В данное понятие входят серверы, компьютеры, планшеты, смартфоны (устройства, операционная система которых позволяет установить САВЗ).

Компьютерный вирус – это программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей без ведома пользователя.

3. Ответственность в системе антивирусной защиты

3.1. Каждый работник МБУК ТМЦ Оренбургского района выполняет роль «пользователя САВЗ».

3.2. Пользователь САВЗ при обнаружении вредоносного кода (получение оповещения САВЗ) обязан:

прекратить (приостановить) свою работу на ОИ;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, а также смежные подразделения, использующие эти файлы в работе;

оценить необходимость дальнейшего использования файлов, зараженных вирусом;

провести «лечение» или уничтожение зараженных файлов. При необходимости для выполнения требований данного пункта следует привлечь администратора антивирусной защиты.

3.3. Пользователю САВЗ запрещается отключать средства антивирусной защиты информации.

3.4. Каждый работник МБУК ТМЦ Оренбургского района несет ответственность за невыполнение или недобросовестное выполнение перечисленных выше обязанностей согласно назначенной роли.

4. Порядок применения средств антивирусной защиты информации

4.1. САВЗ устанавливаются на всех объектах информатизации, эксплуатируемых в МБУК ТМЦ Оренбургского района. При технологической необходимости на отдельные средства вычислительной техники САВЗ могут не устанавливаться, список исключений утверждается начальником МБУК ТМЦ Оренбургского района. САВЗ устанавливается централизованно. Допускаются исключения в централизованной установке, список ОИ, не содержащих САВЗ, утверждается начальником МБУК ТМЦ Оренбургского района.

4.2. Все САВЗ работает в режиме мониторинга в реальном времени. САВЗ проверяют все файлы на локальных и сетевых жестких дисках, съемных носителях, в приложениях к письмам электронной почты, загружаемых из сети Интернет и др., к которым обращается операционная система. Отключение САВЗ допускается только в исключительных случаях.

4.3. Проверка критических областей операционной системы и загрузочных секторов накопителей информации ОИ проводится автоматически САВЗ при каждой загрузке операционной системы.

4.4. Полная проверка всех накопителей информации ОИ проводиться САВЗ автоматически ежемесячно по расписанию.

4.5. В случае наличия признаков вредоносных программ пользователь САВЗ обязан незамедлительно произвести внеплановую полную проверку накопителей информации ОИ и отчуждаемых носителей и создать условия для ее завершения (не извлекать носитель, не останавливать проверку, т.п.).

4.6. Обновление антивирусных баз проводится автоматически не реже одного раза в сутки. Не допускается отключение автоматического обновления САВЗ. В случае невозможности автоматического обновления, обновление баз производится вручную.

4.7. При подключении к ОИ отчуждаемого накопителя информации автоматически проводится полная его проверка на наличие вредоносного кода.

4.8. САВЗ настроено на автоматическое удаление или блокировку исполнения обнаруженного вредоносного кода.

4.9. К использованию в МБУК ТМЦ Оренбургского района допускаются только централизованно закупленные лицензионные САВЗ, распространяемые ответственным за антивирусный контроль.

4.10.В случае необходимости использования сторонних САВЗ, их применение необходимо согласовать.

4.11.При обнаружении вирусов на ОИ, работающем в локальной сети (широковещательном сегменте локальной сети), проверке подлежат все ОИ, включенные в эту сеть и работающие с общими данными и программным обеспечением.

5. Признаки вредоносных программ

5.1. Для проведения полной внеплановой проверки накопителей информации ОИ и отчуждаемых носителей определены следующие признаки вредоносных программ:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача звуковых сигналов системным блоком, не свойственных при обычной работе;
- потеря работоспособности или частые зависания в работе компьютера.

Приложение № 3
к Приказу № 45
от «04» октября 2024 г.

Положение
об использовании сети Интернет в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области

1. Общие положения

Настоящее Положение разработано во исполнение Федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», с учетом ГОСТ Р ИСО/МЭК 27002-2012 «Практические правила управления информационной безопасностью» и устанавливает порядок использовании сети Интернет в Муниципальном бюджетном учреждении культуры «Творческо-методический центр» Оренбургского района Оренбургской области (далее - МБУК ТМЦ Оренбургского района).

Настоящее положение разработано в целях повышения уровня информационной безопасности и эффективности работы сотрудников МБУК ТМЦ Оренбургского района.

Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в МБУК ТМЦ Оренбургского района.

Требования настоящего Положения распространяются на всех сотрудников МБУК ТМЦ Оренбургского района и должны применяться для всех объектов информатизации, эксплуатируемых в МБУК ТМЦ Оренбургского района.

2. Основные термины, сокращения и определения

Адрес IP – уникальный сетевой адрес объекта информатизации в сети, построенной на основе стека протоколов TCP/IP.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.

«белый» ip-адрес – ip-адрес, не принадлежащий диапазону частных адресов и доступный из сети Интернет.

Интернет – компьютерная сеть, представляющая собой глобальную систему соединенных компьютерных сетей, использующих стек протоколов TCP/IP для передачи/обмена данными.

ОИ – объект информатизации, являющийся компонентом ЕИТКС. В данное понятие входят серверы, компьютеры, планшеты, смартфоны, т.п.

ПО – программное обеспечение.

Пользователь – сотрудник МБУК ТМЦ Оренбургского района МБУК ТМЦ Оренбургского района, использующий ресурсы Интернет для выполнения своих должностных обязанностей.

САВЗ – средство антивирусной защиты

Интернет – компьютерная сеть, представляющая собой глобальную систему соединенных компьютерных сетей, использующих стек протоколов TCP/IP для передачи/обмена данными.

NAT – (англ. Network Address Translation – «преобразование сетевых адресов») – это механизм, позволяющий изменять IP-адрес в заголовке сетевого пакета, проходящего через устройство маршрутизации трафика.

VPN (англ. Virtual Private Network «виртуальная частная сеть») – территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, сети Интернет, сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных.

VPN-сервер – узел для построения логической сети.

3. Порядок подключения ОИ к сети Интернет

Для подключения ОИ к сети Интернет сотрудник МБУК ТМЦ Оренбургского района, использующий данный ОИ, должен организовать настройку операционной системы на ОИ и ПО для доступа в Интернет.

ОИ может быть подключен к сети интернет по одному из трех способов:

а) стандартное подключение к сети Интернет;

б) подключение к сети Интернет с повышенной безопасностью;

в) прямое подключение к сети Интернет.

Прямое подключение к сети Интернет осуществляется с назначением ОИ «белого» ip-адреса или с применением технологии преобразования сетевых адресов (NAT).

4. Порядок использования сети Интернет

Доступ в сеть Интернет осуществляется централизованно. На ОИ, подключенному к сети Интернет, в обязательном порядке устанавливается САВЗ, которое эксплуатируется в соответствии с положением по антивирусной защите.

Использование сети Интернет допускается только при выполнении требований положения об антивирусной защите.

Запрещается использовать прямое подключение к сети Интернет, если для выполнения должностных обязанностей и задач достаточно подключения к сети Интернет с повышенной безопасностью или стандартного.

При использовании сети Интернет необходимо:

а) соблюдать требования настоящего Положения;

б) использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;

Перечень типовых угроз при использовании сети Интернет и рекомендации по их предотвращению приведены в Приложении № 1 к Положению.

Общие меры предосторожности при использовании сети Интернет приведены в Приложении № 2 к Положению.

При использовании сети Интернет запрещено:

а) использовать предоставленный МБУК ТМЦ Оренбургского района доступ к сети интернет в личных целях;

б) использовать специализированные аппаратные и программные средства, позволяющие сотрудникам МБУК ТМЦ Оренбургского района получить несанкционированный доступ к сети Интернет;

в) публиковать, загружать и распространять материалы содержащие:

конфиденциальную информацию, а также информацию, составляющую персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является допускает использование сети Интернет;

информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;

вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.;

г) фальсифицировать IP-адрес используемого ОИ, а также прочую служебную информацию;

д) устанавливать на ОИ ПО, не соответствующее требованиям;

е) осуществлять попытки несанкционированного доступа к ресурсам сети Интернет, проведение сетевых атак и сетевого взлома, участие в них, за исключением случаев, если данные действия входят в полномочия сотрудника, проводятся в рамках анализа уязвимостей.

Разрешается устанавливать на ОИ только ПО, соответствующее условиям:

а) ПО является лицензионным. Лицензионное ПО может быть бесплатное (GNU General Public License – лицензия на свободное программное обеспечение);

б) источник ПО должен быть официальным и загружено только: с сайта разработчика; из официальных репозиториев операционных систем; из официальных магазинов приложений;

в) в лицензионном соглашении на ПО не должно быть условий передачи любых данных разработчику или третьим лицам, либо в ПО должна быть

предусмотрена возможность отключения отправки любых данных разработчику или третьим лицам.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО на прокси-сервере и САВЗ на ОИ пользователя.

Информация о посещаемых сотрудниками МБУК ТМЦ Оренбургского района Интернет-ресурсах может протоколироваться для последующего анализа и, при необходимости, предоставляться руководителю МБУК ТМЦ Оренбургского района.

МБУК ТМЦ Оренбургского района имеет право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, несущим угрозу информационной безопасности МБУК ТМЦ Оренбургского района, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

В случае нарушения условий Положения МБУК ТМЦ Оренбургского района вправе, на время проведения проверки и анализа нарушения, отключить ОИ от доступа к сети Интернет, уведомив об этом сотрудника.

Расследование нарушений требований Положения производится в соответствии с положением о реагировании на инциденты информационной безопасности.

5. Ответственность

Сотрудники МБУК ТМЦ Оренбургского района, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами МБУК ТМЦ Оренбургского района.

6. Заключительные положения

Руководитель МБУК ТМЦ Оренбургского района имеет право в целях обеспечения безопасности давать поручения о проведении проверок любого ОИ без предварительного уведомления сотрудников.

Приложение № 1
к Положению об использовании
сети Интернет в МБУК ТМЦ Оренбургского района

Типовые угрозы
при работе с сетью Интернет

№ п/п	Угроза	Примечание	Рекомендуемые меры предосторожности
1.	Заражение компьютера вирусом	чаще всего, заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых»	установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
2.	Заражения компьютера вирусом при просмотре почтовых сообщений	обычно происходит при открытии прикрепленного к письму файла.	не открывать письма, если электронный адрес отправителя не знаком или выглядит «странно»; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
3.	Утечка информации с рабочей станции	уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей). Также причиной утечки может оказаться заражение компьютера вирусом	использовать только лицензионное ПО; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.

4.	Предоставление возможности удаленного управления компьютером	такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом)	использовать только лицензионное ПО; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
5.	Потеря функциональности (полная или частичная) рабочей станции	чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом	использовать только лицензионное ПО; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
6.	Кража личной информации	чаще всего к этому приводит ввод такой информации на веб-страницах (фишинговые страницы), в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам (например, сайту банка), но на самом деле являются подделкой	не открывать письма (и особенно вложения) от незнакомых адресатов; внимательно проверять адрес страницы, на которой вы собираетесь оставить личную информацию; не сохранять пароли в формах веб-страниц и в браузере.
7.	Захват адресов электронной почты, веб-страниц и т.п.	чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу, а также подбор ответа на контрольной вопрос, используемый для восстановления пароля в случае его возможной утери	выполнять требования положения по парольной защите.

Приложение № 2
к Положению об использовании
сети Интернет в МБУК ТМЦ Оренбургского района

Общие меры предосторожности
при работе с сетью Интернет

№ п/п	Мера предосторожности	Примечание
1.	Мониторинг обновлений ПО, используемого на ОИ МБУК ТМЦ Оренбургского района, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.
2.	Приостановка эксплуатацию используемого ПО в случае обнаружения критических, с точки зрения безопасности, уязвимостей и невозможности их устранения.	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих ОИ МБУК ТМЦ Оренбургского района.
3.	При работе с электронной почтой: антивирусная проверка любых прикрепленных файлов перед их запуском или открытием; запрет на открытие писем с вложенными файлами от неизвестных авторов.	Одним из наиболее часто используемых каналов распространения вирусов, а также кражи личной информации, является электронная почта. В случае возникновения вопросов по вложенным файлам во входящих сообщениях электронной почты необходимо обратиться к/в специалисту до принятия решения о дальнейших действиях. Ответственность возлагается на Пользователей.
4.	Запрет автоматического сохранения и/или запуска файлов и элементов	Большинство уязвимостей в программном обеспечении используются через файлы,

	ActiveX, скриптов из сети Интернет на рабочей станции пользователя.	загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код. Для опытных пользователей с разрешения отдела по защите информации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов. Ответственность возлагается на Пользователей.
5.	Запрет на сохранение паролей в заполняемых формах при посещении веб-страниц.	Сохранение пароля может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на Пользователей.