Утверждаю: и.о. директора
МКУ ТГО «Библиотечно-
информационный центр»
_____ Григорьева Л.В.
Приказ № 23
«01» марта 2019г.

Положение

О деятельности Муниципального казённого учреждения «Библиотечно-информационный центр» (МКУ ТГО БИЦ) по обеспечению программно-технической безопасности учреждения и защите детей от информации, причиняющей вред их здоровью и развитию

Раздел 1. Общие положения

1.1. Положение о деятельности Муниципального казённого учреждения «Библиотечно-информационный центр» (далее Учреждения) по обеспечению программно-технической безопасности учреждения и защите детей от информации, причиняющей вред их здоровью и развитию (далее Положение) разработан с на основании ФЗ № 436 "О защите детей от информации, причиняющей вред их здоровью и развитию», ФЗ № 114- «О противодействии экстремистской деятельности», ФЗ № 149 «Об информации, информационных технологиях и защите информации», ФЗ №152«О персональных данных», иными локальными актами Учреждения.

1.2. Положение – документ, определяющий основные принципы организации деятельности, меры, методы, мероприятия, перечень ресурсных средств, правила для сотрудников и пользователей Учреждения, направленных на обеспечению программно-технической безопасности и приоритетной защите детей от информации, причиняющей вред их здоровью и развитию;

1.3. Система обеспечения программно-технической безопасности МКУ ТГО БИЦ состоит из следующих компонентов:

- компьютерная безопасность (компьютеры и программное обеспечение)
- безопасность данных, информационных систем
- безопасность коммуникаций, доступа в интернет

1.4. Обеспечение программно-технической безопасности МКУ ТГО БИЦ осуществляется комплексом технологических и административных мер, применяемых в отношении аппаратных средств, базам данных с целью обеспечения доступности, безопасности, целостности и конфиденциальности информации для пользователей в соответствии с основными принципами деятельности: системности, комплексности, непрерывности защиты, своевременности, преемственности и совершенствования, персональной ответственности.

Раздел 2. Организация деятельности по программно – технической безопасности и защите детей от информации, причиняющей вред их здоровью и развитию

2.1. Использование сети интернет в Учреждении осуществляется в целях:

- обеспечения библиотечно-библиографического, информационного обслуживания населения
- образовательных, учебных

Утверждаю: и.о. директора
МКУ ТГО «Библиотечно-
информационный центр»
_____Григорьева Л.В.
Приказ №_____
«____»_____2019г.

Положение

О деятельности Муниципального казённого учреждения «Библиотечно-информационный центр» (МКУ ТГО БИЦ) по обеспечению программно-технической безопасности учреждения и защите детей от информации, причиняющей вред их здоровью и развитию

Раздел 1. Общие положения

1.1. Положение о деятельности Муниципального казённого учреждения «Библиотечно-информационный центр» (далее Учреждения) по обеспечению программно-технической безопасности учреждения и защите детей от информации, причиняющей вред их здоровью и развитию (далее Положение) разработан с на основании ФЗ № 436 "О защите детей от информации, причиняющей вред их здоровью и развитию», ФЗ № 114- «О противодействии экстремистской деятельности», ФЗ № 149 «Об информации, информационных технологиях и защите информации», ФЗ №152«О персональных данных», иными локальными актами Учреждения.

1.2. Положение – документ, определяющий основные принципы организации деятельности, меры, методы, мероприятия, перечень ресурсных средств, правила для сотрудников и пользователей Учреждения, направленных на обеспечению программно-технической безопасности и приоритетной защите детей от информации, причиняющей вред их здоровью и развитию;

1.3. Система обеспечения программно-технической безопасности МКУ ТГО БИЦ состоит из следующих компонентов:

- компьютерная безопасность (компьютеры и программное обеспечение)
- безопасность данных, информационных систем
- безопасность коммуникаций, доступа в интернет

1.4. Обеспечение программно-технической безопасности МКУ ТГО БИЦ осуществляется комплексом технологических и административных мер, применяемых в отношении аппаратных средств, базам данных с целью обеспечения доступности, безопасности, целостности и конфиденциальности информации для пользователей в соответствии с основными принципами деятельности: системности, комплексности, непрерывности защиты, своевременности, преемственности и совершенствования, персональной ответственности.

Раздел 2. Организация деятельности по программно – технической безопасности и защите детей от информации, причиняющей вред их здоровью и развитию

2.1. Использование сети интернет в Учреждении осуществляется в целях:

- обеспечения библиотечно-библиографического, информационного обслуживания населения
- образовательных, учебных

- получения социально - значимой информации

2.2. Основными направлениями деятельности в Учреждении по обеспечению программно – технической безопасности и приоритетной защите детей от информации, причиняющей вред их здоровью и развитию являются:

- Своевременные оценка, выявление, прогнозирование и устранение источников угроз программно-технической безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования информационно-коммуникационной компьютерной системы учреждения;
- Предоставление доступа пользователей к персональным компьютерам и сети интернет только в соответствии с Правилами пользования библиотеками МКУ ТГО БИЦ, Правилами пользования Центром общественного доступа к сети интернет и электронной информации;
- Разграничение доступа специалистов и пользователей к информационным, аппаратным, программным и иным ресурсам - обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным специалистам и пользователям и в соответствии с ФЗ №436 "О защите детей от информации, причиняющей вред их здоровью и развитию";
- Обеспечение аутентификации (регистрации в учётных документах) пользователей, получающих доступ к компьютерным системам и участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

Раздел 3. Технические меры обеспечения информационной безопасности.

Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ, выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

3.1. В целях предотвращения доступа детей к информации, причиняющей вред их здоровью и развитию на рабочих станциях (ПК) устанавливается система интернет - контроля серверов и локальных фильтров, которая своевременно проходит проверку и при необходимости обновление;

3.2. В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (интернет) осуществляется через компьютеры, с установленными брэндмауэром и антивирусом;

3.3. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней и внешней сетям;

3.4. Запрещена несанкционированная установка программных продуктов

3.5. Подключение рабочих станций к внешним линиям связи производится в локальной вычислительной сети и по протоколам Ethernet и WiFi

Раздел 4. О системном администрировании и разграничение обязанностей ответственных за программно - техническую и информационную безопасность

4.1 Выполнение задач, связанных с мерами системного администрирования, обеспечивающего программно-техническую и информационную безопасность, является частью работы программиста Учреждения.

4.2. Программист Учреждения обязан:

- Следить за соблюдением требований по защите оборудования и информации;
- Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи: антивирусная защита, система контент фильтров;
- Обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей; своевременное обновление программного обеспечения;
- Обеспечивать нормальное функционирование системы резервного копирования;

-Обеспечивать и контролировать физическую целостност (неизменности конфигурации) средств вычислительной техники;

- Осуществлять своевременную проверку программно-технического оборудования и оснащения, контентной фильтрации в соответствии с предъявляемыми требованиями не реже 1 раза в 6 месяцев с составлением акта проверки;

-Предварительно уведомлять руководителей структурных подразделений об отключении серверов или рабочих станций (персональных компьютеров) для технологических целей;

4.3. Во время свободного доступа пользователей к сети Интернет контроль за использованием ресурсов интернета осуществляют работники структурных подразделений, ответственных за данный участок работы. В их обязанности входят:

. - Перед началом использования ПК осуществлять его проверку на наличие обновлённого антивирусного программного обеспечения, работоспособность контент-фильтров, брендмауэра, правильность настроек системного программного обеспечения;

- Проверять все внешние носители информации перед их использованием на ПК на наличие вирусов и опасных программ;

- Ведение «Журнала учёта посещений сети интернет», а также другой учётной документации, и наблюдение за использованием компьютера и сети Интернет;

- Следить за исправностью программно-технического оборудования и своевременно сообщает о неполадках и сбоях программисту Учреждения;

- Проверять и актуализировать список ресурсов внесённых в Единый реестр запрещённых сайтов, в списки экстремистских материалов и применять меры по пресечению обращения пользователей к подобным ресурсам.

- Предотвращать нанесение вреда программно – техническому оснащению и порче имущества;

- Согласовывать действия и обращаться за консультационной помощью по вопросам работы с информационными ресурсами и оборудованием к сотрудникам отделения информационной и библиографической работы МКУ ТГО БИЦ

Библиотечным специалистам запрещено:

- без согласования с программистом учреждения самостоятельно изменять типологию сети, подключать и производить реконфигурацию любого элемента сети, устанавливать новые программные продукты и аппаратные средства, изменяющие настройки операционной системы;

- передавать сторонним лицам какие-либо сведения о настройке элементов сети, операционной системы: пароли, имена пользователей и др.

- при работе с корпоративной электронной почтой открывать файлы, присоединенные к письмам, полученным от незнакомых лиц.

Раздел 5. Правила доступа к сети интернет

5.1. К работе в сети Интернет (локальная точка - рабочая станция или точка коллективного доступа, в том числе по протоколу wi-fi) допускаются лица, прошедшие инструктаж и обязавшиеся соблюдать правила работы в сети интернет, описанные в данном Положении, регламентах, инструкциях и других нормативных документах учреждения.

5.2. Отключение пользователя от сетевых ресурсов производится с обязательным его уведомлением.

5.3. Пользователи имеют право:

- Использовать рабочую станцию (персональный компьютер) и работать в сети интернет в течение периода времени, определенного правилами библиотеки;

- Сохранять полученную информацию на съемном диске (дискете, CD-ROM, флеш-накопителе), предварительно проверенного на отсутствие вирусов;
- Иметь учетную запись в открытых интернет-ресурсах Учреждения;
-Получать консультационную помощь по вопросам работы с персональным компьютером и информационными ресурсами.

5.4. Пользователям запрещается:

- Загружать и распространять материалы, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ;
- Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- Распространять информацию, порочащую честь и достоинство граждан;
- Вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах;
- Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовой страницы браузера);
- Включать, выключать и перезагружать компьютер без согласования с ответственным за ПК;
- Осуществлять, действия, направленные на «взлом» любых компьютеров, находящихся как в точке доступа к интернету учреждения, так и за его пределами;
- Использовать возможности коллективной точки доступа к Интернету для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, экстремистских материалов и информации.

5.5. Пользователи несут ответственность:

- За содержание передаваемой, принимаемой информации;
- За нанесение любого ущерба оборудованию и (порча имущества, вывод оборудования и рабочего состояния) в соответствии с законодательством.

Раздел 6. Контроль и ответственность

6.1. Контроль за соблюдением требований по обеспечению программно - технической и информационной безопасности осуществляют:

- Общий контроль и руководство – руководитель Учреждения. В отделах и отделениях учреждения – руководители структурных подразделений, назначенные приказом ответственными за информационную безопасность;
- Программист – системный администратор в соответствии с обязанностями, указанными в пункте 4.2 данного Положения;
- Библиотечные работники, оказывающие услуги пользователям с помощью программно-технических средств, в соответствии с пунктом 4.3 данного Положения;

6.2. За необеспечение и неисполнение требований по информационной безопасности руководители подразделений, системный администратор, специалисты несут административную и дисциплинарную ответственность в соответствии со своими полномочиями и должностными обязанностями.