Утверждено

Приказом МАУК ЦБС Заиграевского района

от «21» марта 2022 г. № 6

**ИНСТРУКЦИЯ**

**по обеспечению безопасности рабочих мест обработки персональных данных и защите информации**

**муниципального автономного учреждения культуры «Централизованная библиотечная система Заиграевского района**

**1.Общие положения**

* 1. Настоящая инструкция определяет требования по защите персональных данных и определяет систему взглядов на проблему обеспечения комплексной безопасности информации и устанавливает порядок организации и правила обеспечения информационной безопасности в МАУК ЦБС Заиграевского района (далее Учреждение);
  2. Настоящая инструкция определяет распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками, требования по информационной безопасности к информационным средствам, применяемым в Учреждении;
  3. Основополагающим правовым актом в информационной сфере является
  4. закон «Об информации, информатизации и защите информации» (№24-ФЗ от 24.02.95г.) и определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение.

1. **Основные термины, сокращения и определения**
2. **Адрес IP** – уникальный идентификатор АРМ, подключенного к ИС Учреждения, а также сети Интернет.
3. **АРМ** – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.
4. **Интернет** – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
5. **АС** – автоматизированная система Учреждения – система, обеспечивающая хранение, обработку, преобразование и передачу информации Учреждения с использованием компьютерной и другой техники.
6. **ИТ** – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации Учреждения с использованием средств компьютерной и другой техники.
7. **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
8. **ПК** – персональный компьютер.
9. **ПО** – программное обеспечение вычислительной техники, базы данных.
10. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
11. **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
12. **Пользователь** – работник Учреждения, использующий ресурсы Интернет для выполнения своих должностных обязанностей и пользователь Библиотеки, пользующийся услугами Интернет .
13. **Реестр** – документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Учреждения.
14. **Электронная почта** – сервис обмена электронными сообщениями в рамках АС Учреждения (внутренняя электронная почта) и общедоступных сетей Интернет (внешняя электронная почта).

14.**Электронное почтовое сообщение** – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.

15.**Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.

16.**Информационная безопасность** – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

1. **Порядок использования сети Интернет и электронной почты**

3.1. Доступ в сеть Интернет и к электронной почте (далее – к Сервисам) в Учреждении осуществляется централизованно с применением специальных программно-технических средств защиты.

3.2. На АРМ, подключенное к сети Интернет, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.

3.3. При использовании Сервисов необходимо:

3.4.1. Соблюдать требования настоящей Инструкции.

3.4.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.

3.4.3. Ставить в известность Главного библиотекаря ЦОД к сети Интернет и Руководителя и о любых фактах нарушения требований настоящего Положения.

3.4.4. Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении № 1 и обобщенная модель угроз в Приложении № 6.

3.4.5. Общие меры предосторожности при работе с Сервисами приведены в Приложении №2.

3.5. При использовании Сервисов запрещено:

3.5.1. Использовать предоставленный Учреждением доступ к Сервисам в личных целях.

3.5.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам Учреждения получить несанкционированный доступ к Сервисам.

3.5.3. Публиковать, загружать и распространять материалы содержащие:

- конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с руководителем Учреждения и Главным библиотекарем ЦОД к сети Интернет заранее;

-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.

3.5.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

3.5.5. Распространять и устанавливать на служебном ПК любое программное обеспечение и данные, полученные с использованием Сервисов.

3.5.6. Осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.

3.5.7. Переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей.

3.5.8. По собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений, если рассылка не связана с выполнением служебных обязанностей.

3.5.10. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

3.5.11. Публиковать свой электронный адрес, либо электронный адрес других работников Организации на общедоступных не связанных с деятельностью учреждения Интернет-ресурсах (форумы, конференции и т.п.).

3.5.12. Предоставлять работникам Организации (за исключением руководителя Учреждения и Главного библиотекаря ЦОД к сети Интернет) и третьим лицам доступ к своему электронному почтовому ящику.

3.5.13. Перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный.

3.5.14. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам Организации.

3.5.15. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.

3.10. Содержание Интернет-ресурсов, а также файлы, загружаемые из Сервисов, подлежат обязательной проверке на отсутствие вредоносного ПО.

3.11. Информация о посещаемых работниками Организации Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.

3.12. ЦОД к сети Интернет оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.13. Учреждение оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящей Инструкции.

3.15. В случае нарушения пунктов Инструкции Главный библиотекарь ЦОД к сети Интернет вправе отключить АРМ от Сервисов, уведомив об этом руководство структурного подразделения.

* 1. Проводятся плановые проверки состояния информационной

безопасности Главным библиотекарем ЦОД к сети Интернет по защите информации в подразделениях. В ходе плановых проверок должна полностью проверяться вся организация системы информационной безопасности подразделения. Результаты всех проверок оформляются в виде акта с необходимым в каждом конкретном случае приложениями.

3.17. Проверки по фактам нарушения информационной безопасности проводятся ЦОД к сети Интернет и руководством Учреждения после того, как нарушение устранено. Проверка проводится с целью выявление причин и предпосылок нарушения и выработка мер по предупреждению подобных нарушений в дальнейшем.

3.18. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством РФ и локальными нормативными актами Учреждения.

3.19. Под внутренними нарушителями подразумеваются все сотрудники МАУК ЦБС Заиграевского района, имеющие санкционированный доступ на территорию Межпоселенческой центральной библиотеки или к ресурсам автоматизированной системы. Под внешними нарушителями подразумеваются все остальные лица.

**4.Требования по обеспечению безопасности рабочих мест обработки персональных данных и защите информации**

В понятие защиты рабочих мест входит:

4.1. Физическая защита технических средств от несанкционированного доступа:

- регистрация пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

-резервирование технических средств, дублирование массивов и носителей информации;

-использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- использование защищенных каналов связи;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

-организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

-предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

4.2 Парольная защита рабочих мест от несанкционированного доступа к персональных данным:

4.2.1 С целью контроля учетных записей для доступа к информационным ресурсам персональных данных, все легализованные учетные записи ведутся в Журнале учета Логинов (Приложение 3).

4.2.2. Личные пароли доступа создаются пользователями самостоятельно.

4.2.3 Полная плановая смена паролей проводится не реже одного раза в 3 месяца.

4.2.4. Правила формирования пароля:

-Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

-Пароль должен состоять не менее чем из 6 символов.

4.2.5. Лица, использующие паролирование, обязаны своевременно сообщать сотруднику ЦОД к сети Интернет об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4.3. Антивирусная защита рабочих мест от несанкционированного доступа к персональным данным из сети Интернет:

4.3.1. На каждом рабочем месте и серверах должно быть установлено антивирусное программное обеспечение

4.3.2 Антивирусные базы всегда должны быть в актуальном состоянии

4.3.3. Запрещается работа на элементах с выключенным или неработоспособным антивирусным программным обеспечением

4.3.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется Главным библиотекарем ЦОД к сети Интернет в соответствии с руководствами по применению конкретных антивирусных средств. (Приложение 4)

4.3.5. Проверка на наличие вирусов должна проводиться регулярно. Проверке подлежат:

-все файлы на жестких дисках серверов и рабочих мест;

-съемные носители, содержащие персональные данные;

-получаемые из сторонних организаций файлы;

-передаваемые в сторонние организации файлы.

4.3.6. Результаты проверок должны фиксироваться в Журнале антивирусных проверок (Приложение 5).

4.3.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях сотруднику ЦОД к сети Интернет. Сотрудник ЦОД к сети Интернет совместно с пользователем должен выполнить внеочередной антивирусный контроль.

**5.Период действия и порядок внесения изменений в Инструкцию**

5.1 Настоящая Инструкция вводится в действие приказом директора Учреждения.

5.2 Инструкция признается утратившим силу на основании приказа директора Учреждения.

5.3. Изменения в Инструкцию вносятся приказом директора Учреждения.

5.4. Инициаторами внесения изменений в Инструкцию информационной безопасности являются:

- Директор Учреждения;

- Сотрудники, работающие в программе «ИРБИС»

- Главный библиотекарь ЦОД к сети Интернет;

5.5 Плановая актуализация настоящей Инструкции производится ежегодно и имеет целью приведение в соответствие определенных защитных мер реальным условиям и текущим требованиям к защите информации.

5.6 Внеплановая актуализация регламента информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

- при изменении внутренних нормативных документов (инструкций, положений, рекомендаций), касающихся информационной безопасности Департамента;

- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Департамента.

5.7 Ответственными за актуализацию Регламента информационной безопасности (плановую и внеплановую) несет Главный библиотекарь ЦОД к сети Интернет.

5.8. Требования настоящей Инструкции обязательны для всех структурных подразделений Учреждения

Приложение № 1

**Типичные угрозы**

**при работе с сетью Интернет и электронной почтой**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Угроза** | **Примечание** | **Рекомендуемые меры предосторожности** |
|  | Заражение компьютера вирусом. | Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых». | - не посещать перечисленные сайты;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Заражения компьютера вирусом при просмотре почтовых сообщений. | Обычно происходит при открытии прикрепленного к письму файла. | - не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»;  - не открывать прикрепленные файлы, если отправитель письма вам неизвестен;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | 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 принятое к использованию в Учреждении программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | 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 принятое к использованию в Учреждении программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Потеря функциональности (полной или частичной) рабочей станцией. | Чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом. | - использовать только принятое к использованию в Учреждении программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Кража личной информации. | Чаще всего к этому приводит ввод такой информации на веб-страницах, 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. |
|  | 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. | - использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр);  - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию;  - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям;  - не сохранять пароли в формах веб-страниц. |

приложение № 2

**Общие меры предосторожности**

**при работе с сетью Интернет и электронной почтой**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Мера предосторожности** | **Примечание** |
|  | Использование только разрешенногопрограммного обеспечения. | Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО.  Ответственность возлагается на пользователя. |
|  | Отслеживание появления обновлений ПО, используемого на компонентах АС Учреждения взаимодействующих с сетью Интернет. | ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.  Ответственность возлагается на сотрудника ЦОД к сети Интернет |
|  | В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО. | Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.  Ответственность возлагается на пользователей и сотрудника ЦОД к сети Интернет. |
|  | Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Организации, взаимодействующих с сетью Интернет, в режиме мониторинга событий. | Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет.  Ответственность возлагается на сотрудника ЦОД к сети Интернет. |
|  | При работе с электронной почтой – не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку. | В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации – электронная почта.  В случае возникновения вопросов необходимо обратиться в ЦОД к сети Интернет до принятия решения о дальнейших действиях.  Ответственность возлагается на пользователей. |
|  | Запретить автоматическое сохранение и/или запуск файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя. | Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код.  Для опытных пользователей с разрешения сотрудника ЦОД к сети Интернет допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов.  Ответственность возлагается на пользователей. |
|  | Не рекомендуется сохранять пароли в формах при посещении веб-страниц. | Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем.  Ответственность возлагается на пользователей. |

Приложение 3

Форма Журнала учета СЗИ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Уч.№ СЗИ | Наименование СЗИ | Место установки | Дата установки | Подпись установившего | Дата изъятия | Подпись изъявшего |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение № 4

**Форма Журнала учета антивирусных проверок**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Дата проверки | Форма проверки (регулярная/внепланова) | Проверенные АРМ | Результат проверки | Подпись АБ |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Приложение 5

Форма Журнала учета антивирусных проверок

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Дата проверки | Форма проверки (регулярная/внепланова) | Проверенные АРМ | Результат проверки | Подпись АБ |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Приложение № 6

## Обобщенная модель угроз безопасности информации МАУК ЦБС Заиграевского район

| **Угроза информационной безопасности** | **Источник угроз** | **Способы реализации угроз** |
| --- | --- | --- |
| I. Получение информации | 1. Антропогенный | а) Разглашение, передача или утрата атрибутов разграничения доступа |
| б) Внедрение агентов в число персонала системы |
| в) Хищение носителей информации |
| г) Незаконное получение паролей и других реквизитов разграничения доступа |
| д) Несанкционированная модификация программного обеспечения |
| е) Перехват данных, передаваемых по каналам связи |
| ж) Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств |
| II. Анализ характеристик информации | 1. Антропогенный | а) Хищение носителей информации  хищение производственных отходов |
| б) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств |
| в) Несанкционированная модификация программного обеспечения |
| г) Перехват данных, передаваемых по каналам связи, и их анализ |
| III. Изменение (искажение, подмена) информации | 1. Антропогенный | а) Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.) |
| б) Непреднамеренное заражение компьютера вирусами |
| в) Ввод ошибочных данных |
| г) Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования |
| IV. Нарушение информации | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств |
| б) Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.) |
| в) Непреднамеренное заражение компьютера вирусами |
| г) Игнорирование организационных ограничений (установленных правил) при работе в системе |
| д) Ввод ошибочных данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования |
| V. Нарушение работоспособности систем | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств |
| б) Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы |
| 2. Техногенный | а) закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий; |
| б) аварии в системах электропитания; |
| в) аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации; |
| г) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования; |
| д) неумышленное повреждения внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи; |
| е) возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности. |
| 3. Стихийный | а) Разрушение зданий, отдельных помещений |
| б) воздействие атмосферного электричества |
| в) возникновение стихийных очагов пожаров |