УТВЕРЖДЕНА
приказом директора бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя»
от «01» июня 2022 г. № 65
(приложение № 4 к приказу)

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах

I. Общие положения

1.1. Данная Инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных в информационных системах бюджетного учреждения культуры Вологодской области «Вологодский областной театр юного зрителя» (далее – Учреждение).

1.2. Ответственный за обеспечение безопасности персональных данных в информационных системах назначается приказом директором Учреждения.

1.3. Ответственный за обеспечение безопасности персональных данных в информационных системах обладает правами доступа к любым программным и аппаратным ресурсам информационных систем Учреждения.

1.4. Целью защиты информации является:

1.4.1. Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности.

1.4.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности информации, имеющейся в информационных системах Учреждения.

1.4.3. Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.

1.4.4. Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

1.5. Основными видами угроз безопасности защищаемой информации являются:

1.5.1. Противоправные действия третьих лиц.

1.5.2. Ошибочные действия пользователей информационных систем.

1.5.3. Отказы и сбои технических средств информационных систем, приводящие к ее модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

II. Общие обязанности

Ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

2.1. Знать перечень сведений, составляющих защищаемую информацию и условия ее обработки в Учреждении.

2.2. Знать перечень установленных в отделах Учреждения технических средств и перечень задач, решаемых с использованием информационных систем.

2.3. Организовывать определение полномочий пользователей информационных систем (оформление разрешительной системы доступа), минимально необходимых им для выполнения должностных обязанностей.

2.4. Осуществлять оперативный контроль за работой пользователей защищенных автоматизированных рабочих мест и адекватно реагировать на возникающие нештатные ситуации.

2.5. Периодически организовывать проверки актуальности сертификатов соответствия используемых средств защиты информации в информационных системах.

2.6. Блокировать доступ к защищаемой информации при обнаружении нарушений порядка ее обработки.

2.7. Реагировать на попытки несанкционированного доступа к информации в порядке, установленном разделом IV настоящей Инструкции.

2.8. Организовывать установку и настройку средств защиты информации в рамках компетенции.

2.9. По мере необходимости организовывать внесение изменений в конфигурацию технических средств информационных систем, отражать соответствующие изменения в перечне автоматизированных рабочих мест информационной системы.

2.10. Организовывать непосредственное управление и контроль режимов работы функционирования применяемых в информационных системах средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).

2.11. Проводить работу по выявлению возможных каналов утечки информации, изучать текущие тенденции в области защиты персональных данных.

2.12. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами информационных систем, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищенности.

2.13. Организовывать предоставление доступа к информационным системам новым пользователям, предоставлять им возможность задать личный пароль, соответствующий требованиям по организации парольной защиты.

2.14. Организовывать мероприятия по внеплановой смене личных паролей.

2.15. Вносить плановые и внеплановые изменения в учетную запись пользователей информационных систем, в том числе по требованию руководителя структурного подразделения и в случае увольнения работника.

2.16. Организовывать восстановление информации из резервных копий (при наличии) по требованию пользователей информационных систем и в иных случаях, когда это необходимо для восстановления утраченных сведений.

2.17. Хранить дистрибутивы программного обеспечения, установленного в информационных системах, в том числе дистрибутивы средств защиты информации, в месте, исключающим несанкционированный доступ к ним третьих лиц.

2.18. Вносить свои предложения по совершенствованию мер защиты информации в информационных системах, разработке и принятию мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению степени защищенности.

2.19. Знать законодательство Российской Федерации о защите информации, следить за его изменениями.

2.20. Выполнять иные мероприятия, требуемые техническими и программными средствами информационных систем для поддержания их функционирования.

III. Разграничение доступа пользователей к информационным ресурсам и средствам защиты информации

3.1. Защита от несанкционированного доступа осуществляется:

3.1.1. Идентификацией и проверкой подлинности пользователей информационной системы при доступе к информационным ресурсам Учреждения.

3.1.2. Разграничением доступа к обрабатываемым базам данных. Пользователь информационной системы имеет доступ только к тем информационным ресурсам, которые разрешены для него.

3.2. Ответственный за обеспечение безопасности персональных данных в информационных системах должен организовывать мероприятия по обеспечению защиты информационных ресурсов Учреждения от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

IV. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с информационной системой незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, срок действия полномочий которых истек или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к информационной системе, при использовании учетной записи администратора или другого пользователя информационной системы, методом подбора

пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

4.2.1. прекратить несанкционированный доступ к информационной системе;

4.2.2. доложить директору Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

V. Права

Ответственный за обеспечение безопасности персональных данных в информационных системах имеет право:

5.1. Требовать от пользователей информационных систем выполнения инструкций в части работы с программными, аппаратными средствами информационных систем и защищаемой информацией.

5.2. Блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты информации.

5.3. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.

5.4. Производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля.

5.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами информационных систем, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищенности.

VI. Ответственность

6.1. Ответственный за обеспечение безопасности персональных данных в информационных системах несет персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в информационных системах Учреждения, за качество проводимых им работ по обеспечению безопасности защищаемой информации и за все действия, совершенные от имени его учетной записи в информационной системе, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный за обеспечение безопасности персональных данных в информационных системах при нарушении норм, регулирующих получение, обработку

и защиту информации, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

С инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах ознакомлен(а):

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/

«____»______________ 20____ года ________________ /___________________________/