

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 27**

ул. Набережная, 71, хут. Зеленчук Мостовой Отраденского района Краснодарского края,  
352273 ИНН 2345008420 КПП 234501001 ОГРН 1022304448088  
Тел/факс: 8 (86144) 9-86-35 e-mail: school27otr@mail.ru

ПРИНЯТО

На заседании Педагогического совета  
Протокол № 1  
от "30" августа 20 19 г.

УТВЕРЖДЕНО

Приказом директором школы № 63  
от "30" августа 20 19 г.



Р.Т.Тхагалегов

## **ПОЛОЖЕНИЕ**

об информационной безопасности в МБОУ ООШ № 27

хут. Зеленчук Мостовой, 2019 г.

## 1. Общие положения

1.1. Положение об информационной безопасности в МБОУ ООШ № 27 (далее – учреждение) разработано в соответствии с требованиями Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель настоящего Положения - установление надлежащего порядка работы и создание безопасных условий для учащихся и работников учреждения, а также исключения возможности проникновения посторонних лиц, выноса материальных ценностей, иных нарушений общественного порядка.

1.3. Настоящее Положение утверждается директором учреждения и действует на неопределенный срок.

1.4. Изменения и дополнения к настоящему Положению принимаются в порядке, предусмотренном п.1.3. настоящего Положения.

1.5. Положение определяет политику учреждения по безопасности информационных и коммуникационных ресурсов и технологий и общий порядок обращения с документами, содержащими служебную информацию ограниченного распространения.

1.6. В настоящем Положении используются следующие основные термины и понятия:

*Информационный обмен* – процесс передачи и получения информации между пользователями и информационной системой, а также между элементами информационной системы.

*Администратор безопасности* – лицо или группа лиц, ответственных за реализацию мероприятий по защите информации и осуществляющих постоянную организационную поддержку функционирования применяемых средств защиты информации.

*Атака на информационную систему* – любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы.

*Безопасность информации* – защищенность информации от нарушения конфиденциальности, нарушения целостности, утраты или снижения степени доступности, а также незаконного тиражирования.

*Целостность информации* – возможность внесения изменений только авторизованным субъектам доступа.

*Доступность информации* – возможность доступа к информации авторизованного субъекта доступа.

*Внешний воздействующий фактор* – воздействующий на систему фактор, внешний по отношению к объекту информатизации.

*Внутренний воздействующий фактор* – воздействующий на систему фактор, внутренний по отношению к объекту информатизации.

*Вредоносные программы* – программы, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или

нарушению работы.

*Угроза безопасности информации* – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, или пользователю информации.

*Защита информации* – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

*Организационные меры защиты* – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности информации.

*Технические средства защиты* – электронные устройства и специальные программы, выполняющие самостоятельно или в комплексе с другими средствами функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

*Система информационной безопасности* – совокупность организационных мероприятий, технических средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

*Нарушитель* – лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения) и использующее для этого различные возможности, методы и средства.

1.7. Положение устанавливает.

- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности учреждения;
- основные принципы построения системы защиты информации учреждения;
- меры, методы и средства обеспечения информационной безопасности учреждения.

## **II. Цели и задачи системы обеспечения информационной безопасности**

3.1. Субъекты доступа к информации.

*Субъектами доступа к информации* при обеспечении информационной безопасности учреждения являются:

- работники учреждения, участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах учреждения (в соответствии со ст.14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»);
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

3.2. Перечисленным субъектам доступа к информации необходимо обеспечить:

- своевременность доступа к необходимой им информации (ее доступность);
- достоверность (полнота, точность, актуальность, целостность) информации;
- конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;
- возможность осуществления контроля и управления процессами обработки и передачи информации;
- защиту информации от незаконного распространения.

### 3.3. Цели защиты информации.

Основной целью, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных субъектов доступа (устойчивого функционирования системы, при котором авторизованные субъекты доступа имеют возможность получения необходимой информации);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в системах мэрии и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими множеству значимых угроз.

### 3.4. Основные задачи системы обеспечения информационной безопасности учреждения.

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности учреждения должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем учреждения;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования систем мэрии посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам мэрии - обеспечение доступа только к тем ресурсам и

выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;

- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в системах мэрии программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;

- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.5. Основные пути решения задач системы обеспечения информационной безопасности учреждения.

Основные цели обеспечения информационной безопасности и решение перечисленных выше задач достигаются:

- учетом всех подлежащих защите информационных систем учреждения;

- учетом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

- полнотой, реальной выполнимостью и непротиворечивостью требований локальных нормативных актов учреждения по вопросам обеспечения информационной безопасности;

- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;

- наделением каждого работника (пользователя) учреждения минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам учреждения;

- четким знанием и строгим соблюдением всеми пользователями информационных систем учреждения требований локальных нормативных актов учреждения по вопросам обеспечения информационной безопасности;

- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам учреждения;

- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем учреждения;

- применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;

- эффективным контролем над соблюдением пользователями информационных ресурсов учреждения требований по обеспечению информационной безопасности.

## **2. Правовые нормы обеспечения информационной безопасности**

2.1. **Школа имеет право** определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. **Школа обязана** обеспечить сохранность конфиденциальной информации.

### 2.3. *Администрация школы:*

- назначает ответственного за обеспечение информационной безопасности;
- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

### 2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Школы о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Школы и др.

### 2.5. Порядок допуска сотрудников Школы к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и нормативной документации Школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

## **III. Основные угрозы информационной безопасности учреждения**

### 4.1. Существует два вида угроз информационной безопасности:

*Искусственные угрозы* – это угрозы, вызванные деятельностью человека.

*Естественные угрозы* – это угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Наиболее значимыми угрозами информационной безопасности учреждения (способами нанесения ущерба субъектам информационных отношений) являются:

– нарушение функциональности компонентов информационных систем учреждения, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

– нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов учреждения, а также фальсификация (подделка) документов;

– нарушение конфиденциальности (разглашение, утечка) персональных данных.

#### 4.3. Основные источники угроз безопасности информации учреждения:

– непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем учреждения (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;

– преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам учреждения пользователей (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем учреждения;

– удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

– ошибки, допущенные при разработке элементов информационных систем учреждения и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);

– технические сбои элементов информационных систем.

#### 4.4. Пути реализации угроз информационной безопасности учреждения.

4.4.1. Пути реализации непреднамеренных искусственных угроз информационной безопасности учреждения.

Работники учреждения, являющиеся авторизованными субъектами доступа информационных систем, а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации учреждения (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

– неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем учреждения;

– неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

– разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);

– игнорирование установленных правил при работе с информационными ресурсами;

– проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования

информационных систем и информационной безопасности учреждения;

- пересылка информации по ошибочному электронному адресу (устройства); ввод ошибочных данных; неосторожная порча носителей информации; неосторожное повреждение каналов связи;

- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;

- заражение компьютеров вирусами;

- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);

- некомпетентное использование, настройка или неправомерное отключение средств защиты.

Обязанности пользователя информационной системы приведены в Инструкции пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники.

4.4.2. Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности.

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем учреждения из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить):

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем учреждения;
- действия по дезорганизации функционирования информационных систем учреждения, хищение электронных документов и носителей информации;
- несанкционированное копирование электронных документов и носителей информации;
- умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);
- перехват данных, передаваемых по каналам связи и их анализ;
- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);
- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования элементов информационных систем учреждения;
- незаконное использование элементов информационных систем, нарушающее права третьих лиц;
- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.5. Пути реализации основных естественных угроз безопасности информации:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи;
- пожары и стихийные бедствия.

4.6. Модель возможных нарушителей.

4.6.1. Типы нарушителей.

С учетом категории лиц, мотивации, квалификации, наличия специальных средств:

- *некомпетентный (невнимательный) пользователь* – работник учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем учреждения), предпринимающий попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационных систем с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией, действуя по ошибке, некомпетентности или халатности без умысла и использующий при этом только штатные средства;

– *любитель* - работник учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем учреждения), пытающийся нарушить систему защиты без корыстных целей, умысла или для самоутверждения. При этом используются различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств), нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;

– *внутренний (внешний) злоумышленник* - авторизованный субъект доступа (постороннее лицо) действующий целенаправленно (в том числе в сговоре с лицами, не являющимися работниками учреждения). При этом используются методы и средства взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне учреждения.

#### 4.6.2. Внутренние нарушители.

Внутренним нарушителем может быть лицо из следующих категорий работников учреждения:

– зарегистрированные пользователи и персонал, обслуживающий технические средства информационных систем учреждения;

– работники, в том числе руководители, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам учреждения, но имеющие доступ в здания и помещения;

– работники, в том числе руководители, задействованные в разработке и сопровождении программного обеспечения.

#### 4.6.2. Внешние нарушители.

Внешним нарушителем может быть лицо из следующих категорий:

работники учреждения, с которыми прекращен (расторгнут) трудовой договор;

– представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;

– члены преступных организаций или лица, действующие по их заданию;

– лица, случайно или умышленно проникшие в локальную вычислительную сеть учреждения из внешних телекоммуникационных сетей (хакеры).

– администраторы автоматизированных систем учреждения, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям;

– работники учреждения, с которыми прекращен (расторгнут) трудовой договор;

– представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;

– представители внешних организаций, занимающихся разработкой, поставкой,

ремонт и обслуживанием элементов информационных систем;

- члены преступных организаций или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в локальную вычислительную сеть учреждения из внешних телекоммуникационных сетей (хакеры).

- администраторы автоматизированных систем учреждения, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям.

#### 4.7. Утечка информации по техническим каналам.

При проведении мероприятий и эксплуатации технических средств устанавливаются следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств учреждения и линий передачи информации;

- наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети учреждения, на провода и линии, выходящие за пределы контролируемой зоны учреждения, в т.ч. на цепи заземления и электропитания;

- электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом;

- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;

- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;–

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства ("закладки");

- перехват информации или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов мэрии, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими учреждения, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

### **3. Использование сети Интернет**

3.1. Использование сети Интернет в Школе осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам образовательной направленности.

#### **3.2. Работники Школы вправе:**

- размещать информацию в сети Интернет на Интернет-ресурсах Школы;
- иметь учетную запись электронной почты на Интернет-ресурсах Школы.

3.3. **Работникам Школы запрещено** размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства РФ и локальным нормативным актам Школы;
- не относящуюся к образовательному процессу и не связанную с деятельностью Школы;
- нарушающую нравственные и этические нормы, требования профессиональной этики.

#### **3.4. Обучающиеся Школы вправе:**

- использовать ресурсы, размещенные в сети Интернет, в том числе Интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.
- размещать информацию и сведения на Интернет-ресурсах Школы.

#### **3.5. Обучающимся запрещено:**

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;
- осуществлять любые сделки через Интернет;
- загружать файлы на компьютер Школы без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Школы.

3.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием Интернет-адреса (URL) и покинуть данный ресурс.

#### **3.8. Уполномоченное лицо обязано:**

- принять сообщение пользователя;
- принять меры по отключению выхода на данный ресурс с Интернет-ресурсов Школы;
- если обнаруженный ресурс явно нарушает законодательство РФ, сообщить о нем по специальной "горячей линии" для принятия мер в соответствии с законодательством РФ (в течение суток).

#### **3.9. Передаваемая информация должна содержать:**

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ

либо несовместимости с задачами образовательного процесса;

- дату и время обнаружения;
- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

#### **IV. Меры, методы и средства обеспечения информационной безопасности**

##### 6.1. Меры обеспечения информационной безопасности

##### 6.1.1. Законодательные (правовые) меры обеспечения информационной безопасности

К правовым мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем учреждения.

##### 6.1.2. Технологические меры обеспечения информационной безопасности

К данному виду мер обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

##### 6.1.3. Организационные (административные) меры обеспечения информационной безопасности

*Организационные (административные) меры* обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Организационными (административными) мерами обеспечения информационной безопасности являются:

– регламентация доступа в здание учреждения - определяется Положением об организации пропускного режима в МБОУ ООШ № 27;

– регламентация допуска работников к использованию информационных ресурсов - определяется Положением о защите персональных данных работников МБОУ ООШ № 27;

– анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;

– обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники - определяется «Порядком использования средств вычислительной техники»;

– обучение пользователей - регламентируется «Инструкцией пользователя, осуществляющего обработку персональных данных на объектах вычислительной

техники»;

– деятельность по обеспечению информационной безопасности - регламентируется «Положением по обеспечению информационной безопасности»;

– условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами учреждения определяется «Положением о порядке обращения со служебной информацией ограниченного распространения, а также «Положением о защите персональных данных работников МБОУ ООШ № 27», «Положением о защите персональных данных учащихся МБОУ ООШ № 27».

#### 6.1.4. Физические меры обеспечения информационной безопасности

Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

#### 6.1.5. Технические меры обеспечения информационной безопасности

6.1.6. Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

## 4. Мероприятия по обеспечению информационной безопасности

4.1. Для обеспечения информационной безопасности в Школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Школы;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Школы;
- учет всех носителей конфиденциальной информации.

## 5. Организация работы с информационными ресурсами и технологиями

5.1. Система организации делопроизводства:

- учет всей документации Школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

5.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

5.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

5.2.2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

5.2.3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

5.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

5.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы школы.

5.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

5.3. Для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы. Контроль за порядком его ведения возлагается на лицо ответственное за информационную безопасность.

## **6. Обеспечение безопасности на Школьном портале**

6.1. Школьный портал относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

Школьный портал обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в Школьном портале.

6.2. Регламент общих ограничений для участников образовательного процесса при работе со Школьным порталом, обеспечивающей предоставление Услуги:

6.2.1. Участники образовательного процесса, имеющие доступ к Школьному portalу, не имеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам. Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

6.2.2. Участники образовательного процесса, имеющие доступ к Школьному portalу, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

6.2.3. Участники образовательного процесса, имеющие доступ к Школьному portalу, в случае нарушения конфиденциальности условий доступа в личный

кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя Школы, службу технической поддержки Школьного портала (администратора).

6.2.4. Все операции, произведенные участниками образовательного процесса, имеющими доступ к Школьному portalу, с момента получения информации руководителем Школы и службой технической поддержки (администратором) о нарушении, указанном в предыдущем абзаце, признаются недействительными.

6.2.5. При проведении работ по обеспечению безопасности информации на Школьном портале участники образовательного процесса, имеющие доступ к Школьному portalу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

## **7. О системном администрировании и обязанностях ответственного за информационную безопасность**

7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы младшего системного администратора в МБОУ ООШ № 27.

7.2. Для решения задач информационной безопасности системный администратор обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);
- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.

## **8. Антивирусная защита**

8.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

8.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

8.3. За своевременное обновление антивирусного программного обеспечения отвечает младший системный администратор.