

ИНСТРУКЦИЯ
пользователя региональной информационной системы
АИС «Контингент обучающихся»

Условные сокращения:

АИС	- АИС автоматизированная информационная система
АРМ	- автоматизированное рабочее место
ЖМД	- жесткий магнитный диск
ЗИ	- защита информации
НСД	- несанкционированный доступ к информации
ПДН	- персональные данные
ПО	- программное обеспечение
ПЭВМ	- персональная электронно-вычислительная машина
СЗИ	- средство защиты информации
ТЗИ	- техническая защита информации

Настоящая инструкция определяет права и обязанности пользователя в региональной информационной системе АИС «Контингент обучающихся» (далее - АИС).

1. Общие положения

1.1. Пользователь АИС назначается приказом из числа штатных сотрудников, имеющих оформленное разрешение на доступ к защищаемой информации. В части эксплуатации АИС он подчиняется ответственному по обеспечению ТЗИ в АИС и Администратору безопасности АИС.

Назначение и освобождение от исполнения обязанностей согласовывается с ответственным по обеспечению ТЗИ в АИС.

С разрешения директора Гимназии к самостоятельной работе в АИС допускаются пользователи, изучившие настоящую инструкцию.

Процедура регистрации пользователя и предоставления ему прав доступа к ресурсам АИС осуществляется в соответствии с приказами и инструкциями Муниципального бюджетного общеобразовательного учреждения «Гимназия имени А.П.Чехова».

1.2. В практической деятельности пользователь АИС руководствуется следующими документами:

- Федеральный закон от 08.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 28.12.2010 390-ФЗ «О безопасности»
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

- ГОСТ Р 51275 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
- Постановление Правительства РФ от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687
- Эксплуатационно-техническая документация на объекты информатизации.

1.3. Инструкция корректируется и дополняется установленным порядком.

2. Функции пользователя

Основными функциями пользователя АИС являются:

- 2.1. Выполнение мероприятий, направленных на предотвращение непреднамеренного и несанкционированного доступа лиц к защищаемой информации;
- 2.2. Обеспечение режима конфиденциальности при автоматизированной обработке защищаемой информации в АИС;
- 2.3. Автоматизированная обработка защищаемой информации в соответствии с заданием;
- 2.4. Проверка новых данных на отсутствие вирусов.

3. Обязанности пользователя АИС

3.1. Каждый пользователь АИС, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным АИС, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АИС;

хранить в тайне сведения ограниченного доступа, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации;

знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);

хранить в тайне свой пароль (пароли), с установленной периодичностью менять свой пароль (пароли);

использовать для работы, только учтенные накопители информации (каталоги ЖМД, компакт диски и т.д.); контролировать обновление антивирусных баз и в случае

необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту;

присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;

немедленно вызывать ответственного за безопасность информации в автоматизированной системе и ставить его в известность в случае утери индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения; некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных техническим паспортом на ИС отводов кабелей и подключенных устройств.

3.2. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

3.3. Вынос ПЭВМ, на которой проводилась обработка ПДН, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем учреждения запрещен.

3.4. ПЭВМ, используемые для работы с ПДН, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

4. Порядок действий пользователя при работе

4.1. Допуск лиц, работающих с защищаемой информацией, производится установленным порядком. Ответственность за обеспечение защиты информации в процессе эксплуатации объекта информатизации, возлагается на исполнителей, производивших ее обработку, администратора безопасности АИС.

4.2. Обработка (в том числе создание и хранение) защищаемой информации в АИС разрешается только на учтенных машинных носителях информации - ЖМД, флэш-дисках,

оптических накопителях и т.п. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации.

4.3. На период обработки защищаемой информации в помещении, в котором размещаются средства вычислительной техники АИС, могут находиться только лица, наделенные правом самостоятельного доступа в помещение.

4.4. Окна помещений при обработке защищаемой информации должны закрываться шторами (жалюзи).

4.5. Двери в помещения при обработке защищаемой информации должны быть закрыты.

4.6. По окончании обработки защищаемой информации или при передаче управления другому допущенному пользователю необходимо удалить остаточную и не нужную информацию на жестком магнитном диске ПЭВМ и произвести перезагрузку АРМ.

4.7. Работа с СЗИ от НСД осуществляется в соответствии с руководствами пользователя, которые можно найти на официальных сайтах производителей.

4.8. Файлы с защищаемой информацией должны храниться только в установленных для этого каталогах (разделах) - защищаемых ресурсах.

4.9. Уничтожение файлов, машинных носителей содержащих защищаемую информацию, осуществляется по акту о стирании информации соответствующего уровня конфиденциальности, уничтожении машинных носителей информации, машинных документов.

4.10. Распечатка любой защищаемой информации на печатающем устройстве производится в соответствии с утвержденной организационно-распорядительной документацией.

5. Общий порядок работы пользователя.

5.1. Получить у ответственного по обеспечению ТЗИ в АИС персональный пароль под роспись, при первоначальном доступе к АИС.

5.2. Выполнить предусмотренные организационно-технические мероприятия по ЗИ.

5.3. Включить ПЭВМ, убедиться в исправности и нормальном функционировании.

При появлении приглашения на ввод пароля ввести с клавиатуры свой индивидуальный пароль и нажать клавишу <Enter>.

5.4. Для доступа к системе следует ввести в адресной строке браузера 10.62.50.157 и нажать клавишу <Enter>.

5.5. Зайти под своим логином и паролем и выполнить работу согласно заданию.

5.6. Сообщить при необходимости о нештатных ситуациях, фактах вскрытия ПЭВМ администратору безопасности информации.

5.7. Выключить ПЭВМ.

5.8. Пользователям запрещается:

- Использовать компоненты программного и аппаратного обеспечения в неслужебных целях;
- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами АРМ;
- Осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации;
- Оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- Передавать кому-либо свой пароль (кроме ответственного за информационную безопасность или руководителя организации);
- Оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);
- Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность ответственного за безопасность информации.

6. Ответственность

6.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. За разглашение конфиденциальной информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Ответственный за защиту персональных данных:

⋮

С инструкцией ознакомлен:

СОСТАВ

рабочей группы по внедрению в МБОУ «Гимназия им. А.П.Чехова» Регионального сегмента межведомственной системы учета Контингент обучающихся по основным образовательным программам и дополнительным общеобразовательным программам
(АИС «Контингент обучающихся»)

Руководитель рабочей группы:

Венжик Тамара Дмитриевна заместитель директора по УВР

Члены рабочей группы:

Черепова Ольга Николаевна учитель информатики

Никульшин Евгений Николаевич техник-программист

Грибова Светлана Николаевна секретарь руководителя

План мероприятий по внедрению в МБОУ «Гимназия им. А.П.Чехова» автоматизированной
информационной системы «Контингент обучающихся»

п/п	Наименование мероприятия	Сроки реализации	Ответственные
1.	Утверждение нормативной и иной документации гимназии по внедрению и ведению АИС «Контингент обучающихся»	до 01.02.2017	Директор Подзорова Е.А.
2.	Создание всех необходимых условий для внедрения и обеспечения работы системы	до 01.04.2017	Директор Подзорова Е.А.
3.	Формирование рабочей группы по внедрению АИС «Контингент обучающихся»	до 01.02.2017	Директор Подзорова Е.А.
4.	Определение координатора внедрения АИС «Контингент обучающихся» в гимназии	01.02.2017	Директор Подзорова Е.А.
5.	Разработка плана мероприятий по внедрению АИС «Контингент обучающихся»	01.01.2017	Директор Подзорова Е.А.
6.	Семинар с педагогическим составом по внедрению АИС «Контингент обучающихся» в гимназии	до 01.04.2017	Директор Подзорова Е.А.
7.	Подключение к АИС «Контингент обучающихся»	до 01.04.2017	Техник-программист Никульшин Е.Н.
8.	Информирование педагогической и родительской общественности о внедрении АИС «Контингент обучающихся», в т.ч. через средства массовой информации.	до 01.05.2017	Заместитель директора по УВР Венжик Т.Д., техник-программист Никульшин Е.Н.
9.	Организация работы всех типов пользователей (сотрудников, учащихся и родителей) на уровне гимназии.	до 01.09.2017	Заместитель директора по УВР Венжик Т.Д.
10.	Управление правами доступа в систему; контроль полноты, качества и оперативности ведения информации в системе	Постоянно	Заместитель директора по УВР Венжик Т.Д.
11.	Консультирование классных руководителей и педагогического состава гимназии по работе с АИС «Контингент обучающихся»	Постоянно	Заместитель директора по УВР Венжик Т.Д.

12.	Первичное наполнение и выверка данных АИС «Контингент обучающихся», обеспечение качества и достоверности информации, вводимой в АИС «Контингент обучающихся»	до 01.09.2017	Классные руководители, педагоги, учитель информатики Черепова ОН.
13.	Своевременное ведение электронной книги движения учащихся (зачисление в гимназию, выбытие из гимназии, переводы из класса в класс)	В течение учебного года	Секретарь Грибова СМ.
14.	Формирование базы данных внутри гимназических электронных документов (локальные акты, приказы и т.п.)	В течение учебного года	Секретарь Грибова С.Н.
15.	Обеспечение взаимодействия с ПАО «Ростелеком» по вопросам технического сопровождения внедрения АИС «Контингент обучающихся»	По мере необходимости	Техник-программист Никульшин Е.Н., учитель информатики Черепова ОН.
16.	Информирование Роскомсвязи о внесении изменений в порядок работы с персональными данными	По мере необходимости	Техник-программист Никульшин Е.Н., учитель информатики Черепова ОН.
17.	Заключение сопутствующих договоров на внедрение АИС «Контингент обучающихся»	По мере необходимости	Заместитель директора по АХР Гаус Р.Р.
18.	Внесение изменений в локальные акты гимназии	Апрель - август 2017	Директор Гимназии Подзорова Е.А.
19.	Внесение изменений в должностные инструкции сотрудников гимназии	до 01.09.2017	Инспектор ОК Грибова С.Н.