КОМИТЕТ КОМИТЕТА г.СЛАВГОРОДА АЛТАЙСКОГО КРАЯ
ПО ОБРАЗОВАНИЮ

П Р И К А З

02 августа 2013 г. № 267

Об утверждении Положения об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

В соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», п. 2.4. Решения совместного заседания Совета при Губернаторе Алтайского края по вопросам защиты информации и Постоянно действующей технической комиссии Администрации Алтайского края по защите государственной тайны от 29 июня 2012 года и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой и защитой информации, п р и к а з ы в а ю:

1.Утвердить прилагаемое Положение об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию.

2. Положение разместить на официальном сайте Комитета администрации г.Славгорода Алтайского края по образованию.

3. Контроль исполнения настоящего приказа возложить на ведущего специалиста по информатизации Комитета администрации г.Славгорода Алтайского края по образованию Дмитриева А.А.

Председатель Комитета Л.В. Подгора

Дмитриев А. А.

ПРИЛОЖЕНИЕ
УТВЕРЖДЕНО
приказом Комитета
администрации
г.Славгорода Алтайского края
по образованию
от 02 августа 2013 N 267

ПОЛОЖЕНИЕ
об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Положение об обеспечении безопасности общедоступной информации при ее обработке в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - Положение) разработано согласно Решения Совета при Губернаторе по вопросам защиты информации от 29.06.2012 в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой и защитой информации.

1.2. Настоящее положение устанавливает требования к обеспечению безопасности общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС), доступ к которой не ограничен федеральными законами.

Под ИС понимается - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, расположенных в кабинетах Комитета администрации г.Славгорода Алтайского края по образованию по адресу: г. Славгород, ул.К-Либкнехта 136.

ИС используются для хранения, обработки и передачи информации, в соответствии с функциями, возложенными на Комитет администрации г.Славгорода Алтайского края по образованию.

ИС включает в себя: рабочие станции, сетевое оборудование, периферийное оборудование (принтеры, сканеры и т.п.) и другое специализированное оборудование Комитета администрации г.Славгорода Алтайского края по образованию.

1.3. Безопасность общедоступной информации, при ее обработке в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию, обеспечивается применением организационных мер и технических средств защиты информации, реализующих требования нормативных правовых актов Российской Федерации.

1.4. Требования настоящего Положения и других документов, разработанных для их реализации, являются обязательными для исполнения всеми лицами, получившими доступ к общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию, и должны быть доведены до их сведения.

1.5. Решение о необходимости внесения изменений в Положение принимается на основании:

-изменения нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации;

-результатов анализа инцидентов информационной безопасности в информационных системах;

изменения технологии обработки информации.

1.6. Изменения настоящего Положения подлежат предварительной оценке до их ввода в действие, на соответствие нормативным правовым актам Российской Федерации, регулирующим отношения, связанные с обработкой и защитой информации.

2. Цель защиты информации и основные виды угроз безопасности.

2.1. Основной целью Положения является обеспечение принятия организационных и технических мер, направленных на:

-обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении такой информации;

-реализацию права на доступ к информации.

2.2. На основании Положения устанавливаются требования:

-разграничения доступа к общедоступной информации, порядка и условий такого доступа;

-обработки информации;

-передачи информации другим лицам по договору или на ином установленном законом основании.

2.3. Основными видами угроз безопасности общедоступной информации в ИС являются:

-противоправные и (или) ошибочные действия пользователей информационных систем и третьих лиц;

-отказы, сбои программного обеспечения и технических средств информационных систем, приводящие к модификации, блокированию, уничтожению, а также нарушению правил эксплуатации ПЭВМ;

-стихийные бедствия, техногенные аварии, сбои и отказы технических средств информационных систем.

3. Методы и способы защиты общедоступной информации в ИС.

3.1. Для достижения основной цели защиты информации, системы безопасности информации обеспечивают эффективное решение следующих задач:

-предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

-своевременное обнаружение фактов несанкционированного доступа;

-предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

-недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

-возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

-постоянный контроль за обеспечением защищенности информации.

3.2.Для выполнения требований настоящего Положения утверждаются:

-инструкция по проведению антивирусного контроля в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (Приложение 1);

-инструкция по предоставлению доступа к информационным системам Комитета администрации г.Славгорода Алтайского края по образованию (Приложения 2 и 3);

-инструкция по организации парольной защиты в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (Приложение 4);

-инструкция по организации технического обслуживания и ремонта технических средств в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (Приложение 5);

-инструкция по работе пользователей в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (Приложение 6);

-инструкция по организации резервного копирования в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (Приложения 7).

3.3.Охрана помещений, в которых ведется обработка информации и организация режима безопасности в этих помещениях, обеспечивает сохранность технических средств ИС, носителей информации и средств защиты информации, а также исключение возможности неконтролируемого пребывания посторонних лиц в этих помещениях.

4. Обязанности.

4.1. Специалист по информатизации Комитета администрации г.Славгорода Алтайского края по образованию:

-сопровождает функционирование программного обеспечения рабочих станций ИС;

-организует техническое обслуживание рабочих станций, периферийного и другого специализированного оборудования Комитета администрации г.Славгорода Алтайского края по образованию;

-организует работы по проведению антивирусного контроля рабочих станций;

-отвечает за соблюдение в ИС требований по обеспечению безопасности информации;

-отвечает за своевременное обнаружение фактов несанкционированного доступа к ИС;

-разрабатывает предложения по дальнейшему совершенствованию системы защиты информации, планируют мероприятия по защите ИС.

4.2. Пользователь ИС - сотрудник, допущенный к работе в ИС:

-отвечает за соблюдение установленного порядка использования программного обеспечения, а также применение технических и программных средств ИС;

-соблюдает требования нормативных документов по обеспечению безопасности информации, обрабатываемой в ИС;

-не имеет права на изменение компонентов ПЭВМ, отключение или изменение настроек антивирусной защиты.

5. Ответственность.

5.1. Ответственность за реализацию и соблюдение требований Положения пользователями ИС, возлагается на начальников структурных подразделений и сотрудников Комитета администрации г.Славгорода Алтайского края по образованию.

5.2. Нарушение требований Положения влечет за собой дисциплинарную, административную и иную ответственность в соответствии с действующим законодательством Российской Федерации.

6. Заключительные положения.

6.1. Настоящее Положение вступает в силу с момента его утверждения и действует без ограничения срока действия.

6.2. Настоящее Положение не заменяет собой нормативные правовые акты Российской Федерации.

Приложение 1
к Положению об обеспечении
безопасности общедоступной
информации в информационных системах
Комитета администрации г.Славгорода
Алтайского края по образованию

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет порядок обеспечения антивирусной защиты в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС).

1.2. В целях обеспечения антивирусной защиты в ИС производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля рабочих станций Комитета администрации г.Славгорода Алтайского края по образованию возлагается на специалиста по информатизации.

1.4. К применению в ИС допускается лицензионное антивирусное программное обеспечение.

2. Порядок проведения антивирусного контроля рабочих станций.

2.1. Установка и настройка средств антивирусного контроля на рабочих станциях ИС Комитета администрации г.Славгорода Алтайского края по образованию осуществляется специалистом по информатизации.

2.2. Антивирусный контроль осуществляется на рабочих станциях в постоянном режиме.

2.3. Обновление баз антивирусного ПО производится автоматически на периодической основе.

2.4. В начале работы при включении, а также при доступе к файлам в автоматическом режиме проводится их антивирусный контроль. Один раз в неделю, в автоматическом режиме производится полная проверка рабочей станции на наличие вирусов.

2.5. При работе со съемными носителями информации пользователи ИС перед началом работы осуществляют их антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по каналам связи общего пользования.

2.6. При возникновении подозрения на наличие вируса, пользователь ИС самостоятельно, или вместе со специалистом по информатизации, проводит внеочередной антивирусный контроль ПЭВМ.

2.7. При обнаружении вируса пользователь ИС приостанавливает работу на ПЭВМ и сообщает специалисту по информатизации.

2.8. Пользователь ИС совместно со специалистом по информатизации проводит лечение зараженных файлов с помощью антивирусного ПО и после этого повторно проводит антивирусный контроль.

2.9. В случае обнаружения на ПЭВМ не поддающегося лечению вируса, прекращается работа на ПЭВМ и принимаются меры по восстановлению ее работоспособности.

3. Порядок проведения антивирусного контроля в серверной группе.

3.1. Установка и настройка средств антивирусного контроля на серверах ИС Комитета администрации г.Славгорода Алтайского края по образованию осуществляется специалистом по информатизации.

3.2. Антивирусный контроль осуществляется на серверах в постоянном режиме.

3.3. Обновление баз антивирусного ПО проводится автоматически на периодической основе.

3.4. В начале работы при включении, а также при доступе к файлам в автоматическом режиме проводится их антивирусный контроль. Один раз в неделю, в автоматическом режиме производится полная проверка серверов на наличие вирусов.

3.5. При работе со съемными носителями информации специалист по информатизации перед началом работы осуществляет их антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по каналам связи общего пользования.

3.6. При возникновении подозрения на наличие вируса, специалист по информатизации самостоятельно проводит внеочередной антивирусный контроль сервера.

3.7. При обнаружении вируса специалист по информатизации проводит лечение зараженных файлов с помощью антивирусного ПО и после этого вновь проводит антивирусный контроль.

3.8. В случае обнаружения на сервере не поддающегося лечению вируса, принимаются меры по восстановлению работоспособности ИС.

Приложение 2
к Положению
об обеспечении безопасности
общедоступной информации в
информационных системах Комитета
администрации г.Славгорода Алтайского
края по образованию

ИНСТРУКЦИЯ
по предоставлению доступа к информационным системам Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет правила предоставления доступа к информационным системам Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС).

1.2. К работе с ИС допускаются пользователи, ознакомленные с Положением по защите общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - Положение) и нормативными документами, разработанными для реализации требований данного Положения.

1.3. Каждому сотруднику, допущенному к работе с информационными системами, создается учетная запись пользователя ИС, под которой он будет регистрироваться и работать в ИС.

1.4. В случае необходимости сотрудникам могут быть предоставлены несколько учетных записей. Использование несколькими сотрудниками одной и той же учетной записи ЗАПРЕЩЕНО.

2. Порядок создания (продления) учетной записи пользователя ИС, предоставления (изменения) полномочий, удаления учетной записи пользователя ИС.

2.1. Процедура регистрации (создания) учетной записи пользователя ИС, блокирования учетной записи, а также предоставления (или изменения) прав доступа пользователя ИС к информационным ресурсам для сотрудника инициируется заявкой начальника подразделения (отдела), в котором работает данный сотрудник (Приложение 3).

Устные указания о допуске кого бы то ни было к ИС, не имеют силы и не обязательны для исполнения.

2.2. Заявку на имя специалиста по информатизации Комитета администрации г.Славгорода Алтайского края по образованию подписывает начальник подразделения (отдела). В заявке указывается: должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника, а также список информационных ресурсов, к которым необходимо предоставить доступ.

2.3. На основании заявки специалист по информатизации Комитета администрации г.Славгорода Алтайского края по образованию совершает необходимые операции по созданию (удалению) учетной записи пользователя ИС, присвоению ему начального значения пароля и прав доступа к информационным ресурсам ИС.

По окончании в заявке делается отметка о выполнении за подписями исполнителей.

2.4. В случае окончания срока действия полномочий сотрудника (окончание договорных отношений, увольнение) учетная запись пользователя ИС должна блокироваться.

Приложение 3
к Положению об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

(форма заявки)

Специалисту по информатизации
Комитета администрации г.Славгорода
Алтайского края по образованию

_____
(Ф.И.О.)

_____

ЗАЯВКА

На создание (изменение, удаление) учетной записи пользователя ИС

Прошу создать (изменить, удалить) учетную запись пользователя:
(нужное подчеркнуть)

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Учетная запись (если есть)	
Ф.И.О. непосредственного руководителя, должность, телефон	

Прошу предоставить доступ к следующим ресурсам:

Локальная сеть	
Internet	
Правовые системы	
Адрес электронной почты (e-mail)	
(указать нужное)	

Председатель Комитета _____ _____ "___" _____ 20 __г.
(Ф.И.О.) (подпись)

С правилами работы в информационной системе Комитета администрации г.Славгорода Алтайского края по образованию ознакомлен:

_____ _____ " ___ " _____ 20 __ г.
(Ф.И.О.) (подпись)

_____ _____
(назначенная учетная запись пользователя ИС) (адрес электронной почты)

Приложение 4
к Положению об обеспечении
безопасности общедоступной
информации в информационных
системах Комитет администрации
г.Славгорода Алтайского края
по образованию

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет основные правила генерации, смены и прекращения действия паролей (удаления учетных записей пользователей ИС) в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС), а также контроль за действиями пользователей ИС и обслуживающего персонала системы при работе с паролями.

1.2. Контроль за действиями пользователей ИС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на специалиста по информатизации.

1.3. Идентификация и аутентификация пользователей в ИС осуществляется посредством использования персональных учетных записей пользователей ИС и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

-пароль содержит не менее шести символов;

-не является словом, присутствующим в словарях, или профессиональным термином;

-не содержит легко угадываемые последовательности.

1.4. Временный пароль, создаваемый при заведении учетной записи или смене забытого пароля, должен передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем ИС при первом обращении к ИС. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации.

2. Порядок генерации, смены, прекращения действия и резервирования паролей.

2.1. Производится резервирование некоторых паролей, таких, как пароли администраторов ИС, пароли ответственных должностных лиц, пароли отдельных пользователей ИС, выполняющих важные функции, пароли обеспечивающие работу отдельных сетевых сервисов.

2.2. Блокирование учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) производится специалистом по информатизации после окончания последнего сеанса работы данного пользователя с ИС.

2.3. В случае компрометации пароля пользователя ИС проводится внеплановая смена пароля.

3. Пользователю ИС запрещается:

-сообщать свой пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей учетных записей);

-сохранять пароль в программно-технических средствах в открытом виде;

-использовать учетные записи других лиц.

Приложение 5
к Положению об обеспечении
безопасности общедоступной
информации в информационных
системах Комитета администрации
г.Славгорода Алтайского края по
образованию

ИНСТРУКЦИЯ
по организации обслуживания технических средств и сопровождения программного обеспечения в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет общие принципы организации обслуживания и ремонта технических средств, сопровождения программного обеспечения (далее - ПО), устранения неисправностей работы ПО и технических средств в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС).

1.2. Ответственность за поддержание установленного в настоящей Инструкции порядка сопровождения аппаратно-программного комплекса рабочих станций, периферийного оборудования и других технических средств ИС Комитета администрации г.Славгорода Алтайского края по образованию возлагается на специалиста по информатизации.

2. Обслуживание и ремонт технических средств в ИС.

2.1. Обслуживание технических средств ИС организуется в целях предотвращения неисправностей, обеспечения работоспособности компонентов ИС.

2.2. При проведении технического обслуживания (далее - ТО) и ремонта необходимо руководствоваться следующими правилами:

-обслуживание технических средств ИС в соответствии с рекомендациями производителя;

-выполнение ТО и ремонта только уполномоченным персоналом ИС;

-принятие соответствующих мер защиты информации в ИС на период выполнения ТО и ремонта (в случае необходимости, информация должна быть удалена);

-соблюдение требований, устанавливаемых гарантийными обязательствами производителя технических средств.

2.3. Для обслуживания технических средств ИС проводятся следующие виды ТО:

-ежедневное обслуживание;

-ежемесячное обслуживание;

-ежегодное обслуживание.

2.4. Процедура ежедневного ТО включает в себя:

-визуальный осмотр технических средств ИС;

-очистка поверхности элементов устройств от пыли и грязи;

-проверка состояния соединительных кабелей и разъемов.

Ежедневное обслуживание технических средств, размещенных на рабочих местах пользователей ИС, выполняют пользователи ИС, а других средств - уполномоченный персонал ИС.

2.5. Ежемесячное и ежегодное ТО проводятся в соответствии с эксплуатационной документацией технического средства.

Ответственность за своевременное проведение еженедельного и годового ТО, ремонта возлагается на уполномоченный персонал ИС.

3. Сопровождение программного обеспечения ИС.

3.1. Поддержка и сопровождение ПО ИС заключается в выполнении следующих видов работ:

-установка ПО;

-настройка и адаптация установленного ПО;

-установка обновлений ПО;

-устранение неисправностей, связанных с использованием установленного ПО;

-консультирование пользователей ИС.

3.2. При сопровождении ПО в ИС уполномоченный персонал ИС руководствуется следующими правилами:

-выполнение работ по сопровождению ПО уполномоченным персоналом ИС;

-выполнение требований лицензионных соглашений на использование ПО в соответствии с законодательством Российской Федерации;

-руководство документацией разработчиков при сопровождении ПО;

-при использовании сертифицированного по требованиям безопасности информации ПО, осуществление его настройки и поддержки в соответствии с техническими условиями или формуляром;

-при участии в сопровождении сторонних организаций принятие дополнительных мер по исключению несанкционированного доступа к информации в ИС;

-ограничение возможности изменения пользователем ИС состава и настроек ПО ИС, если это не противоречит эксплуатационной документации.

4. Устранение неисправностей технических средств и программного обеспечения ИС.

4.1. Уполномоченный персонал ИС обеспечивает анализ и устранение неисправностей технических средств и ПО, принимает соответствующие действия по их предупреждению.

4.2. После выявления неисправности, отказа технических средств и ПО уполномоченным персоналом или специалистами сторонних организаций (при гарантийном обслуживании) выполняются необходимые работы по восстановлению работоспособности: ремонт, замена составных частей, автономные и комплексные проверки, переустановка настройка ПО, консультирование пользователей ИС.

Приложение 6
к Положению об обеспечении
безопасности общедоступной
информации в информационных
системах Комитета администрации
г.Славгорода Алтайского края по
образованию

ИНСТРУКЦИЯ
по работе пользователей в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет общие принципы работы пользователей в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС) при обработке общедоступной информации. Пользователи ИС несут персональную ответственность за свои действия.

1.2. Допуск пользователей ИС к работе с ИС осуществляется в соответствии с «Инструкцией предоставления доступа к информационным системам Комитета администрации г.Славгорода Алтайского края по образованию».

2. Порядок работы пользователей в ИС.

2.1. Пользователь ИС имеет право в рабочее время решать поставленные ему задачи в соответствии с полномочиями доступа к ИС.

2.2. Пользователь ИС отвечает за правильность включения и выключения ПЭВМ, входа в ИС и действия при работе в ИС.

2.3. Вход пользователя в ИС осуществляется под учетной записью пользователя ИС, созданной в соответствии с «Инструкцией предоставления доступа к информационным системам Комитета администрации г.Славгорода Алтайского края по образованию». Требования к паролю и периодичности его замены установлены в «Инструкции по организации парольной защиты в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию».

2.4. В случае отказа ИС в идентификации пользователя, либо не подтверждения пароля следует обратиться к специалисту по информатизации.

2.5. Перед началом работы со съемными носителями информации пользователь ИС обязан проверить их на наличие вирусов с использованием антивирусного ПО, установленного в ИС, в соответствии с «Инструкцией по проведению антивирусного контроля в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию». В случае обнаружения вирусов пользователь ИС обязан сообщить специалисту по информатизации.

3. Ограничения в работе пользователя ИС.

3.1. В процессе работы пользователю ИС запрещается: осуществлять попытки несанкционированного доступа к ресурсам ИС; подменять своими действиями функции администратора по изменению полномочий доступа к ресурсам ИС;

-оставлять ПЭВМ с незавершенным сеансом. При отсутствии визуального контроля за ПЭВМ доступ к ПЭВМ должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>; допускать посторонних лиц к ПЭВМ;

-сообщать (или передавать) посторонним лицам аутентифицирующую информацию;

-самостоятельно устанавливать, или модифицировать ПО, непосредственно не связанное со служебной деятельностью;

-изменять установленный алгоритм функционирования технических средств или программного обеспечения ИС;

-работать на ПЭВМ при обнаружении неисправности; вносить изменения в конструкцию, конфигурацию, размещение ПЭВМ и другие узлы ИС;

-использовать ресурсы ИС для осуществления деятельности не связанной со служебными обязанностями;

-предпринимать какие-либо действия, направленные на нарушение работы сетевого оборудования и разрушение ресурсов ИС.

4. Ответственность.

4.1. Ответственность за допуск пользователя к ресурсам ИС и установленные ему полномочия несет руководитель структурного подразделения.

4.2. Пользователи ИС, нарушившие требования Положения по защите общедоступной информации в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию, несут дисциплинарную, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации и внутренними организационно-распорядительными документами.

4.3. По всем возникающим вопросам при работе в ИС необходимо обращаться к специалисту по информатизации.

Приложение 7
к Положению
об обеспечении безопасности
общедоступной информации в
информационных системах
Комитета администрации
г.Славгорода Алтайского края по
образованию

ИНСТРУКЦИЯ
по организации резервного копирования в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию

1. Общие положения.

1.1. Данная инструкция определяет порядок организации резервного копирования информации, обрабатываемой в информационных системах Комитета администрации г.Славгорода Алтайского края по образованию (далее - ИС), меры и средства поддержания непрерывности работы и восстановления работоспособности ИС.

1.2. Инструкция описывает:

-мероприятия по защите ИС от потери информации;

-действия по восстановлению информации ИС.

1.3. Действие настоящей инструкции распространяется на администратора безопасности ИС и пользователей ИС.

2. Порядок реагирования на Инциденты.

2.1. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а так же потерей информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

-в результате действий пользователей ИС или третьих лиц;

-в результате нарушения правил эксплуатации технических средств ИС;

-в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки специалистом по информатизации принимаются меры по восстановлению работоспособности ИС. Предпринимаемые меры в случае необходимости согласуются с руководством.

3. Меры по обеспечению непрерывности работы и восстановления ресурсов при возникновении инцидентов.

3.1. Для предотвращения потерь информации при отключении электроэнергии, все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также ПЭВМ подключаются к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

-локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных ПЭВМ;

-источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

-дублированные системы электропитания в устройствах (сетевое оборудование, ПЭВМ и т.д.).

3.2. Для защиты от неисправностей носителей информации на ПЭВМ, осуществляющих обработку и хранение информации, рекомендуется использовать резервирование информации при помощи технологии RAID (кроме RAID-0).

3.3. Система резервного копирования и хранения информации обеспечивает хранение защищаемой информации на носителе, не участвующем в обработке информации.

3.4. Резервное копирование и хранение информации осуществляется на периодической основе.

3.5. Носители информации, на которые произведено резервное копирование, учитываются соответствующим образом.

3.6. Для обеспечения возможности восстановления информации, носители хранятся не менее года.