УТВЕРЖДАЮ
Директор Гимназии № 63
О.Г.Туманова
приказ №273 от 31.12.2011г.

ИНСТРУКЦИЯ
администратора безопасности информации в ГБОУ Гимназии №63 Калининского района Санкт-Петербурга

1. Общие положения

Данная Инструкция является руководящим документом администратора безопасности информации ГБОУ Гимназии № 63.

Требования настоящей инструкции должны выполняться во всех режимах функционирования структурного подразделения.

Требования администратора безопасности, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками структурного подразделения.

Конфиденциальная информация относится к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для автоматизированных систем (АС) являются:

- несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;

- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

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

Работа с конфиденциальной информацией (в том числе со служебны документами ограниченного распространения, персональными данными т.д.) строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени каждый документ (не зависимо от типа носителя: бумажный, электронны должен отвечать и распоряжаться конкретный работник, выдача документ осуществляется только под роспись;

- принцип контроля и учета – все операции с документами должн отражаться в соответствующих журналах и карточках (передача из рук руки, снятие копии и т.п.).

2. Назначение администратора безопасности структурного подразделения

На должность администратора безопасности назначается лицо из числ наиболее квалифицированных пользователей ПЭВМ структурног подразделения, в котором эксплуатируется информационная система.

Администратор безопасности в вопросах защиты информации взаимодействует с сотрудниками отдела по защите информации Правительства области.

3. Обязанности администратора безопасности структурного подразделения

В своей повседневной деятельности администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту конфиденциальной информации от утечки по техническим каналам и НСД, эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации (СЗИ НСД) и от утечки информации по техническим каналам.

Администратор безопасности совместно со специалистами по информационным технологиям и защите информации:

- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;

- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;

- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации (устойчивое функционирование ЛВС и ее подсистем).

На администратора безопасности возлагаются следующие обязанности:

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах ПЭВМ;

- знать уровень конфиденциальности обрабатываемой информации, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации;

- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации;

- совместно со специалистами по информационным технологиям и защите информации обеспечивать доступ к защищаемой информации структурного подразделения пользователям согласно их прав доступа;

- незамедлительно докладывать руководителю подразделения, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;

- контролировать правильность применения пользователями сети средств защиты информации;

- участвовать в испытаниях и проверках АС;

- не допускать к работе на рабочих станциях и серверах структурного подразделения посторонних лиц;

- осуществлять контроль монтажа оборудования структурного подразделения специалистами сторонних организаций;

- участвовать в приемке для нужд структурного подразделения новых программных средств;

- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;

- при изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС, обрабатывающей информацию ограниченного доступа;

- вести журнал учета работы с автоматизированной системо обрабатывающей информацию ограниченного доступа.

Регистрации в журнале учета работ АС, обрабатывающей информаци ограниченного доступа подлежат:

- обновление программного обеспечения АС;

- обновление антивирусных баз;

- вскрытие системного блока с целью модернизации или ремонта указанием цели вскрытия и проводимых работ;

- создание резервной копии базы данных и пр. служебной информации

- замена системного блока с указанием факта гарантированног удаления информации с жесткого магнитного диска;

- отклонения в нормальной работе системных и прикладны программных средств затрудняющих эксплуатацию рабочей станции;

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);

- перебои в системе электроснабжения;

- и.т.п.

При выявлении нарушения первой категории (утечка информации) администратор обязан немедленно прекратить работы на АС.

При выявлении нарушений первой, второй и третьей категорий администратор обязан подать служебную записку руководству и занести соответствующую запись в журнал учета работы АС с изложением факта нарушения, предпринятые и/или рекомендуемые им действия.

Форма журнала регистрации работ АС (образец заполнения):

Дата	Наименование работ	Ф.И.О. исполнителя работ	АС № ___	Роспись
1	2	3	4	5
01.02.2005	Обновление антивирусной базы, сканирование дисков	ФИО	АС №1 – АС №6	

02.01.2005	Переустановка операционной системы	ФИО	АС №3	
09.02.2005	Замена манипулятора мышь	ФИО	АС №7	
14.02.2005	Резервное копирование информации: «КАДРЫ», «Мои документы»	ФИО	 АС №4 АС №1 – АС №6	

3. Ответственность

Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на его в соответствии с настоящей Инструкцией и другими нормативными документами по защите информации.