ПОЛОЖЕНИЕ **об информационной безопасности** **в ОГКОУ КШИ «Колпашевский кадетский корпус»**

Термины и определения

Рабочая станция – персональный компьютер, предназначенный для доступа пользователей к ресурсам Автоматизированной системы учреждения, приема, передачи и обработки информации.

Автоматизированная система (АС) – совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки информации.

Системный администратор – должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса учреждения, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных.

Учетная запись – информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.). Пароль – секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

1 Назначение и область применения

1.1 Положение об информационно безопасности Областного государственного казённого общеобразовательного учреждения кадетской школы-интернат «Колпашевский кадетский корпус» (далее – Положение, учреждение) регламентирует порядок организации и правила обеспечения информационной безопасности в колледже, распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками учреждения, требования по информационной безопасности к информационным средствам, применяемым в учреждении.

1.2 Положение является локальным нормативным актом учреждения. Требования настоящего Положения обязательны для всех структурных подразделений учреждения.

1.3 Положение утверждается приказом директора учреждения в установленном порядке.

2 Цели и задачи обеспечения безопасности информации

2.1 Главная цель обеспечения безопасности информации, циркулирующей в учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту – конфиденциальной или защищенной информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы учреждения.

2.2 Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в учреждении;
- предотвращение нарушений прав личности обучающихся, работников учреждения на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3 Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам учреждения, нарушению нормального функционирования и развития учреждения;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- координация деятельности структурных подразделений учреждения по обеспечению защиты информации;

3 Организация системы обеспечения информационной безопасности

3.1 Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы учреждения;
- средства телекоммуникаций;
- помещения;
- сотрудников учреждения.

3.2 В целях реализации стоящих перед системой обеспечения информационной безопасности задач в учреждении устанавливаются:

- защита персональных данных персонала и обучающихся;
- контроль за использованием электронных средств информационного обеспечения деятельности учреждения;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности учреждения электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- принятие мер к воспрепятствованию доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- проверка целесообразности использования персоналом и обучающимися учреждения интернет – ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- обучение персонала учреждения по вопросам обеспечения информационной безопасности;
- контроль за правильностью использования имеющихся в учреждении средств телефонной связи;
- защита персональных данных персонала и обучающихся – мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся учреждения при их обработке с использованием средств автоматизации или без использования таких средств;
- контроль за использованием электронных средств информационного обеспечения деятельности учреждения по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности учреждения электронных носителей информации способных произвести заражение программного обеспечения вирусами – контроль за используемым программным обеспечением и проверка его подлинности;
- обучение персонала учреждения по вопросам обеспечения информационной безопасности – проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению информационной безопасности учреждения.

3.3 Общее руководство системой информационной безопасности учреждения осуществляет директор учреждения.

4 Учетные записи

4.1 Локальные учетные записи компьютеров, связанные с учебным процессом (Admin, Guest), предназначены для служебного использования системным администратором при настройке системы и не предназначены для повседневной работы.

4.2 Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях, связанных с учебным процессом, при первоначальном конфигурировании операционной системы.

4.3 Для повседневной работы, связанной с учебным процессом, должны быть созданы локальные учетные записи без прав администратора (Кадет, Кабинет-7 и т.п.).

5 Доступ к ресурсам Интернет

5.1 Для использования задач, связанных с производственной деятельностью сотрудникам учреждения, предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях запрещен;

5.2 Доступ к ресурсам Интернет может быть заблокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами;

5.3 Правила работы персонала и обучающихся учреждения в компьютерных сетях приведены в приложении 1;

5.4 Правила работы с ресурсами Интернет приведены в приложении 2.

6 Антивирусная защита

6.1 К использованию в учреждении допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств;

6.2 Установка средств антивирусного контроля на компьютерах учреждения осуществляется уполномоченными сотрудниками;

6.3 Настройка параметров средств антивирусного контроля осуществляется уполномоченными сотрудниками в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

6.4 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), а так же информация на съемных носителях.

6.5 Антивирусная проверка должна проводиться:

- на компьютерах сотрудников – не реже одного раза в неделю;
- на серверах – не реже двух раз в неделю;

6.6 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с системным администратором должен провести внеочередной антивирусный контроль своей рабочей станции.

7 Установка и обслуживание оборудования, программ

7.1 Установка и обслуживание оборудования возможна только уполномоченными сотрудниками и системным администратором. Установка и обслуживание оборудования сотрудниками других отделов запрещена.

7.2 Установка программ возможна только уполномоченными сотрудниками и системным администратором. Установка программ сотрудниками других отделов запрещена.

Правила работы персонала и обучающихся учреждения в компьютерных сетях

1 Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети учреждения и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников учреждения. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности учащихся.

2 Основными принципами политики учреждения для работы в Сетях являются:

- равный доступ для всех обучающихся;
- использование Сетей обучающимися только для образовательных целей;
- защита обучающихся от вредной или незаконной информации, содержащей: порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.

3 Полномочия преподавателей и сотрудников.

3.1 Системный администратор:

- организует и руководит всей деятельностью по реализации настоящих Правил;
- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями учреждения;
- обеспечивает контроль за соблюдением правил работы обучающихся в сетях;
- незамедлительно сообщает директору о выявленных нарушениях и принимает меры по устранению нарушений.

3.2 Преподаватели классов, в которых установлены компьютеры, обязаны:

- объяснить обучающимся правила безопасного и ответственного поведения при работе в Сетях;
- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания;
- осуществлять непрерывный контроль работы обучающихся в Сетях;
- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;
- немедленно сообщать системному администратору, директору или уполномоченному сотруднику о нарушении правил или о создании незаконного контента в сети учреждения;
- не покидать учебный кабинет во время урока, и не допускать обучающихся во время перемены к работе в Сетях;

3.3 Преподаватели несут ответственность за целостность оборудования учреждения, закрепленного за учебным кабинетом, в котором проводят занятия.

4. Права и обязанности обучающихся

4.1 Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации учреждения;
- на получение доступа к сети Интернет (только под наблюдением преподавателя);
- на грамотное и ответственное обучение работе в Сетях;

4.2 Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;
- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;
- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;
- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети учреждения или атаки на другие системы;

- запрещено использование нелегального программного обеспечения, защищенного авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

5 Ответственность

5.1 Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка учреждения;

5.2 Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

Приложение 2

Правила работы с ресурсами сети Интернет

1.1 Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Системный администратор и уполномоченные сотрудники имеют право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

1.2 При работе с ресурсами сети Интернет недопустимо:

1.2.1 разглашение коммерческой и служебной информации учреждения, ставшей известной сотруднику учреждения по служебной необходимости либо иным путем;

1.2.2 распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну или прочие права собственности;

1.2.3 публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ. Для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

1.3 При работе с ресурсами Интернет запрещается:

1.3.1 загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

1.3.2 использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

1.4 Возможность получить доступ к ресурсу не является гарантией того, что запрашиваемый ресурс является разрешенным политикой учреждения.