Инструкция пользователя по обеспечению информационной безопасности в Рудненском индустриальном институте.

1.Общие положения

1.1. Настоящая инструкция устанавливает порядок действий преподавателей, сотрудников и студентов при работе с ресурсами и сервисами сети Интернет.

1.2. Ознакомление с инструкцией и ее соблюдение обязательны для всех преподавателей, сотрудников и студентов образовательного учреждения, а также иных лиц, допускаемых к работе с ресурсами и сервисами сети Интернет.

2. Организация использования сети Интернет в образовательном учреждении

2.1. Доступ к информационным ресурсам несовместимым с целями и задачами образования и воспитания студентов запрещен.

2.2. При использовании сети Интернет преподавателями, сотрудниками и студентами предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Республики Казахстан и которые имеют прямое отношение к образовательному процессу.

2.3. При использовании ресурсов сети обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

2.4. При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

2.5. Все компьютеры, подключаемые к сети Интернет, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

3. Права, обязанности и ответственность пользователей

3.1. Использование ресурсов сети Интернет осуществляется в целях образовательного процесса.

3.2. Сотрудники могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию работы сети Интернет и ограничению доступа.

3.3. К работе в сети Интернет допускаются лица, ознакомившиеся с настоящей инструкцией и обязавшиеся соблюдать правила работы.

3.4. Пользователям запрещается:

-посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Республики Казахстан (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

-загружать и распространять материалы, содержащие 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 сети Интернет, а также размещение ссылок на выше указанную информацию;

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

-распространять информацию, порочащую честь и достоинство граждан;

-осуществлять любые сделки через сеть Интернет;

-работать с объемными ресурсами (видео, аудио, чат, фото) без согласования с лицом, назначенным ответственным за организацию работы в сети Интернет.

3.5. Пользователи несут ответственность:

-за разглашение пароля, выдаваемого для работы с информационными ресурсами РИИ. При смене пароля, он должен состоять не менее чем из 6 символов, содержать минимум одну заглавную букву и одну строчную на латинском языке. Не желательно чтобы пароль содержал год рожденя или имя;

-за содержание передаваемой, принимаемой и печатаемой информации;

-за нанесение любого ущерба оборудованию (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность в соответствии с законодательством;

3.6. Пользователи имеют право:

-работать в сети Интернет в течение периода времени;

-сохранять полученную информацию на съемном диске (дискете, CD, флеш-накопителе).

4. Действия во внештатных ситуациях

4.1. При утрате (в том числе частично) подключения к сети Интернет лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за организацию подключения к сети Интернет.

5. С целью обеспечения компьютерной безопасности пользователь обязан:

5.1 Держать включённым антивирусное программное обеспечение на компьютере. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.

5.2 Ежедневно проверять состояние антивирусного программного обеспечения, а именно:

5.2.1. обеспечить постоянное включение режима автоматической защиты;

5.2.2 дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;

5.2.3 просматривать журналы ежедневных антивирусных проверок;

5.2.4 контролировать удаление вирусов при их появлении.

5.2.5 Не реже одного раза в месяц посещать сайт http://windowsupdate.microsoft.com и проверять, установлены ли последние обновления операционной системы.

5.2.6 Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.

5.2.7 В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.