C=RU, O=ГБПОУ ОГТ им.В.И.Суркова, CN=Захаров Н_В_, E=ogt-surkova@yandex.ru
00e94f8928bb4a3aad
2023-01-26 13:21:17

УТВЕРЖДАЮ
Директор ГБПОУ «Обшаровский государственный техникум им.В.И.Суркова»
Приказ № 44/о/д от 19.01.2023г.
_____ Н.В.Захаров
«19» января 2023г.

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАССМОТРЕНО
Советом обучающихся
Протокол № 5 от 19.01.2023г.

РАССМОТРЕНО
Советом родителей
Протокол № 5 от 19.01.2023г.

Термины и определения

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы техникума.

Рабочая станция - персональный компьютер (терминал), ноутбук, моноблок, предназначенный для доступа пользователей к ресурсам сети «Интернет», приема, передачи и обработки информации.

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

Пользователь - сотрудник техникума, использующий ресурсы информационной системы техникума для выполнения должностных обязанностей.

Учетная запись - информация о 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.

Изменение полномочий - процесс создания удаления, внесения изменений в учетные записи пользователей рабочих станций, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю рабочей станции.

1. Назначение и область применения

1.1. Положение об информационной безопасности Государственного бюджетного профессионального образовательного учреждения Самарской области «Обшаровский государственный техникум им. В.И.Суркова» (далее - Положение, техникум) регламентирует порядок организации и правила обеспечения информационной безопасности в техникуме, распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками техникума, требования по информационной безопасности к информационным средствам, применяемым в техникуме.

1.2. Положение является локальным нормативным актом техникума.

Требования настоящего Положения обязательны для всех структурных подразделений техникума и распространяются на:

- рабочие станции;

- средства телекоммуникаций;

- помещения;

- сотрудников техникума.

1.3. Положение утверждается приказом директора техникума в установленном порядке.

2. Общие положения

2.1. Информационная безопасность является одним из составных элементов комплексной безопасности техникума. Под информационной безопасностью техникума понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

2.2. Информационная безопасность - деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов автоматизированных и телекоммуникационных систем, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

2.3. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба. Информационная безопасность включает:

- защиту интеллектуальной собственности техникума;

- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;

- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;

- учет всех носителей конфиденциальной информации.

2.4. Информационная безопасность техникума должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

- целостность (точность и полноту информации и компьютерных программ);

- доступность (возможность получения пользователями информации в пределах их компетенции).

2.5. К объектам информационной безопасности техникума относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных,

осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

2.6. Правовую основу Положения составляют:

- Конституция Российской Федерации;

- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;

- Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;

- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;

- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ (в ред. от 27.07.2011)

- ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 № 447-ст)

- другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

3. Цели и задачи обеспечения безопасности информации

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

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в техникуме;

- предотвращение нарушений прав личности обучающихся, работников техникума на сохранение конфиденциальности информации;

- предотвращение несанкционированных действий по блокированию информации;

3.3. 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 техникума, нарушению нормального функционирования и развития техникума;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- координация деятельности структурных подразделений техникума по обеспечению защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота.

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности

- создание механизмов управления системой информационной безопасности (СИБ).

4. Организация системы обеспечения информационной безопасности

4.1. Система обеспечения информационной безопасности распространяются на:

- рабочие станции техникума;

- средства телекоммуникаций;

- помещения;

- сотрудников техникума.

4.2. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в техникуме устанавливаются:

- защита персональных данных персонала и обучающихся;

- контроль за использованием электронных средств информационного обеспечения деятельности техникума по прямому назначению;

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности техникума нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

- внутрисетевой контроль за перемещением информации;

- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

- проверка целесообразности использования персоналом и обучающимися техникума интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;

- обучение персонала техникума по вопросам обеспечения информационной безопасности;

- контроль за правильностью использования имеющихся в техникуме средств телефонной и радиосвязи;

- защита персональных данных персонала и обучающихся - мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся техникума при их обработке с использованием средств автоматизации или без использования таких средств;

- контроль за использованием электронных средств информационного обеспечения

деятельности техникума по прямому назначению - плановые и внеплановые проверки в структурных подразделениях техникума. Содержание проверок - сложившаяся практика использования персональных компьютеров, мультимедийных систем, интерактивных средств обучения, телевизионных приемников, копировально-множительной аппаратуры и сканирующих устройств, электронных средств проектирования и инженерной графики, телефонных аппаратов и радиостанций, а также программного обеспечения к указанным средствам и устранение выявленных в ходе проверок недостатков.

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности техникума нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами - контроль за используемым программным обеспечением и проверка его подлинности, ограничение в использовании съемных и компакт-дисков сотрудниками и обучающимися техникума;

- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими

постоянное ознакомление со сведениями об информационных материалах признанных в соответствии с действующим законодательством экстремистскими, доведение этих сведений до администрации и персонала техникума и принятие мер к воспрещению доступа к этим материалам (мерами технического противодействия - в отношении материалов находящихся в сети Интернет, и путем изъятия - в отношении печатных изданий, хранящихся в библиотеке техникума);

- проверка целесообразности использования персоналом и обучающимися техникума интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия - установление и доведение в форме инструкций до персонала и обучающихся техникума общедоступных требований об ограничениях при использовании ресурса, предоставляемого им администрацией техникума, постоянный контроль за выполнением указанных ограничений, разработка, внедрение, и применение технических (программных) средств противодействия возникающим нарушениям, либо злоупотреблениям;

- обучение персонала техникума по вопросам обеспечения информационной безопасности - проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению ин формационной безопасности техникума.

- контроль за правильностью использования имеющихся в техникуме средств телефонной и радиосвязи - выявление фактов нецелевого использования средств телефонной и радиосвязи и принятие мер технического и организационного характера по их недопущению.

4.3. Общее руководство системой информационной безопасности техникума

осуществляет системный администратор. Руководители структурных подразделений техникума обязаны участвовать в ее поддержании в надлежащем состоянии, дальнейшем развитии и совершенствовании по своим направлениям деятельности.

5. Порядок обеспечения информационной безопасности

5.1. Организационное и техническое обеспечение рабочего процесса сотрудников возлагается на системного администратора

5.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с рабочей станцией, должно быть сопоставлено персональное уникальное имя - учетная запись пользователя и пароль, под которым он будет работать в системе.

5.3. Проведение операций, указанных п. 4.2. сотрудниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

5.4. Правила работы сотрудников техникума и обучающихся в компьютерных сетях приведены в Приложении 1.

6. Требования к паролям

6.1. Пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику техникума, используемая для подтверждения подлинности владельца учетной записи.

6.1.1. Установку пароля производит пользователь при первом входе в систему с новой учетной записью.

6.1.2. При выборе пароля необходимо руководствоваться следующими правилами:

- длина пароля должна составлять не менее 8 символов;

- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;

- запрещается использовать в качестве пароля название учетной записи, фамилию или имя пользователя, а также легко угадываемые сочетания символов.

6.1.3. Пользователь несет персональную ответственность за сохранение в тайне своего пароля. Запрещается сообщать пароль другим, записывать его, а также пересылать открытым текстом в электронных сообщениях.

6.1.4. Пользователь обязан не реже одного раза в три месяца производить смену основного пароля, соблюдая требования настоящего Положения.

6.1.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом инженеру-программисту и изменить

пароль.

7. Доступ к ресурсам Интернет

7.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам техникума предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях запрещен.

7.2. Требуемый уровень доступа предоставляется сотруднику техникума на основании заявки на имя директора техникума.

7.3. Доступ к ресурсам Интернет может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

7.4. Правила работы с ресурсами Интернет приведены в Приложении 1.

8. Электронная почта

8.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам техникума предоставлен доступ к системе электронной почты.

8.2. Электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

8.3. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководства.

8.4. В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы системы электронной почты, системный администратор обязан немедленно сообщить об этом директору для принятия решений.

8.5. Правила работы с электронной почтой приведены в Приложении 3.

9. Антивирусная защита

9.1. К использованию в техникуме допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

9.2. Установка средств антивирусного контроля на компьютерах (серверах ЛВС) техникума осуществляется уполномоченными сотрудниками.

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

9.4. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС

- при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов РС.

9.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CO-КОМ и т.п.).

9.6. Антивирусная проверка должна проводиться:

- на компьютерах сотрудников - не реже одного раза в неделю;

- на серверах ЛВС - не реже двух раз в неделю

9.7. 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.

10. Хранение данных

10.1. Служебная информация сотрудников техникума должна храниться в специально отведенных папках на серверах ЛВС техникума. Хранение служебной информации на компьютерах сотрудников запрещено.

10.2. Для хранения личной информации сотрудников возможно выделение сетевых папок согласно заявке «На внесение изменений в списки пользователей». Хранение личной информации в служебных папках запрещено.

10.3. Для обеспечения целостности данных необходимо проводить резервное копирование не реже одного раза в сутки сотрудниками отдела АСУ. Резервное копирование личной информации сотрудниками отдела АСУ не предусмотрено.

10.4. Ответственность:

10.4.1. Ответственность за обеспечение целостности данных, хранимых на серверах техникума в соответствии с требованиями настоящего положения возлагается на начальника отдела АСУ.

10.4.2. Ответственность за обеспечение целостности данных, хранимых на локальных компьютерах сотрудников техникума в соответствии с требованиями настоящего Положения возлагается на самих сотрудников.

11. Установка и обслуживание оборудования

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

11.1.1. Ответственность за сбои в работе оборудования лежит системном администраторе

12. Установка и обслуживание программ

12.1. Установка программ возможна только системным администратором. Установка программ сотрудниками других отделов запрещена.

12.2. Ответственность за сбои в работе программ лежит на системном администраторе

Приложение 1

Правила

работы персонала и обучающихся техникума в компьютерных сетях

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

2. Основными принципами политики техникума 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. Правила работы в Сетях должны быть расположены в каждом компьютерном классе.

4. Полномочия преподавателей и сотрудников.

4.1. 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 техникума;

- создает возможности для обогащения и расширения образовательного процесса через Сети;

- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;

- обеспечивает контроль за соблюдением правил работы обучающихся в сетях;

- предоставляет технические возможности в области мониторинга трафика, передаваемого через Сеть техникума;

- организует в начале каждого учебного года ознакомление обучающихся с правилами безопасной работы в Сети. Информирует обучающихся, что трафик контролируется;

- организует поддержку и обновление сайта. Размещает на сайте только материалы, утвержденные директором;

- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений;

4.2. Преподаватели компьютерных классов обязаны:

- объяснять 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 и приводить перечень соответствующих интернет-адресов;

- осуществлять непрерывный контроль работы обучающихся в Сетях в учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;

- немедленно сообщать системному администратору или директору о нарушении правил или о создании незаконного контента в сети техникума;

4.3. Преподаватели несут ответственность за целостность оборудования техникума, закрепленного за учебным кабинетом, в котором проводят занятия.

5. Права и обязанности обучающихся

5.1. Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации техникума;

- на получение доступа к сети Интернет (только под наблюдением преподавателя);

- на грамотное и ответственное обучение работе в Сетях;

- быть информированным о правилах работы в Сетях.

5.2. 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.;

- не должны отправлять или отвечать на сообщения, оскорбительные, угрожающие или непристойные;

- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети техникума или атаки на другие системы;

- запрещается использование чужих имен пользователя, пароля и электронной почты;

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

6. Ответственность

6.1. Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка техникума.

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

6.3. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ и РС (Я).

Приложение 2

ПРАВИЛА

работы с ресурсами сети Интернет

1.1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Системный администратор техникума имеет 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 техникума, ставшей известной сотруднику техникума по служебной необходимости либо иным путем;

1.2.2. распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

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 организации.

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

1.5. Вся информация о ресурсах, посещаемых сотрудниками техникума,

протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также администрации техникума для детального изучения.

Приложение 3

Правила работы с электронной почтой

1. Служебный адрес электронной почты является собственностью техникума и может быть использован только в служебных целях. Использование электронной почты в других целях категорически запрещено.

2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

3. При работе с системой электронной почты сотрудникам техникума запрещается:

3.1. использовать адрес служебной почты для оформления подписок и массовых рассылок;

3.2. публиковать свой адрес, либо адреса других сотрудников техникума на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

3.3. открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

3.4. осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;

3.5. осуществлять массовую рассылку почтовых сообщений рекламного характера;

3.6. рассылка через электронную почту 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 Интернете, а также ссылки на вышеуказанную информацию;

3.7. распространение защищаемых авторскими правами материалов, затрагивающих какой- либо патент, торговую марку, коммерческую тайну,

копирайт или прочие права собственности и/или авторские и смежные с ним права третьей сторон;

3.8. распространять информацию содержание и направленность которой 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. распространять информацию ограниченного доступа, представляющую коммерческую тайну;

3.9. предоставлять кому бы то ни было пароль для доступа к своему почтовому адресу.