«Согласовано»
на заседании Педагогического Совета
Протокол № 4
от 13 февраля 2018 г.

«Утверждаю»
Директор ГБПОУ «ТКСиТ»
Е.А. Кузнецова
Приказ № 56-08
от 15 марта 2018 г.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ (ИКС) ГБПОУ «ТКСиТ»

1. Общие положения

1. Настоящее положение разработано в целях обеспечения защиты информации и упорядочивания доступа к ней, руководствуясь статьями 16 и 17 Закона Российской Федерации от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации", Устава ГБПОУ «ТКСиТ»
2. Настоящее Положение определяет структуру и управление ИКС, порядок использования оборудования ИКС, организацию подключения к ИКС и организацию доступа к электронным информационным ресурсам ИКС, порядок защиты информации в ИКС.
3. Положение обязательно для исполнения всеми сотрудниками и обучающимися колледжа, имеющими доступ в ИКС.
4. Основными целями создания ИКС являются:

1) повышение эффективности работы сотрудников и студентов колледжа за счет внедрения информационных, и коммуникационных технологий;
2) предоставление сотрудникам и студентам колледжа доступа к электронным информационным ресурсам образовательного учреждения;
3) обеспечение пользователей ИКС корпоративным доступом в сеть Интернет и электронной почтой;
4) централизованное обеспечение информационной безопасности образовательного учреждения;
5) оптимизация расходов образовательного учреждения на информатизацию.

5. В настоящем Положении используются следующие термины и определения:

1) Microsoft Windows Server - служба файлового сервера, обеспечивающая поддержку иерархической структуры ИКС, наращиваемость и расширяемость, а также функции распределенной безопасности;
2) домен - базовая организационная структура Microsoft Windows Server, представляющая собой административную единицу;
3) Сетевой диск - назначенный логический диск, который служит для хранения "общих" файлов, доступных для всех пользователей, на других персональных компьютерах (далее - ПК), включенных в общую локальную сеть;

4) каталог (папка, директория) - объект в файловой системе, упрощающий организацию файлов. Типичная файловая система содержит большое количество файлов, и каталоги помогают упорядочить ее путем их группировки;

5) база данных - объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины;

6) инженер-электроник - сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения, а также обеспечение информационной безопасности в организации;

7) средства вычислительной техники (далее - СВТ) - персональные компьютеры, мобильные компьютеры, серверное оборудование, принтеры, сканеры, а также другое оборудование ИКС, предназначенное для сбора и подготовки, ввода, накопления, обработки, вывода, отображения, приема и передачи информации;

8) информационно-коммуникационная сеть (далее - ИКС) - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. ИКС состоит из линий связи, коммуникационного оборудования, средств вычислительной техники и другого оборудования, обеспечивающего функционирование прикладного и системного программного обеспечения ИКС, а также обработку, передачу, хранение и накопление информации, предоставляемой и распространяемой с использованием данной сети;

9) ресурсы ИКС - совокупность данных, файловых, сетевых и вычислительных ресурсов и информационных систем ИКС;

10) информационная система - совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

11) несанкционированный доступ к информации - получение пользователем доступа к информации, разрешение на доступ к которой в соответствии с принятой политикой безопасности отсутствует;

12) пользователь ИКС - сотрудник образовательной организации, подключенный к ИКС, и имеющий учетную запись, пароль в операционных системах, системах управления базами данных, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, имеющий доступ к аппаратным средствам, программному обеспечению (далее - ПО);

13) локальная вычислительная сеть (далее - ЛВС) - объединенные в общую информационную сеть с помощью специального коммуникационного оборудования средства вычислительной техники, расположенные на незначительном удалении одно от другого, с целью совместной работы и доступа к информации;

14) сервер - вычислительная система, предоставляющая общий доступ к своим ресурсам (вычислительным, дисковым, программным) пользователям ИКС или программ. Необходимость установки сервера обусловлена потребностью доступа к сходным информационным ресурсам, централизацией информации, ее накоплением и необходимостью ее быстрой обработки;

15) спам - массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений (информации) лицам, не выражавшим желания их получать.

2. Структура и управление ИКС

1. Физически ИКС состоит из соединенных каналами связи локальных вычислительных сетей учебных и административных кабинетов, обязательно подключаемых к ИКС.
2. Логическая структура ИКС базируется на Microsoft Windows Server.
3. Главной логической структурной единицей ИКС является домен образовательного учреждения.
4. Управление структурой, серверами и коммуникационным оборудованием ИКС осуществляется исключительно инженерами-электрониками образовательного учреждения и обслуживающей сервера организацией.
5. Инженер-электроник разрабатывает инструкции, определяющие:
1) правила работы с электронной почтой в образовательном учреждении;
2) порядок настройки, использования ПО и СВТ;
3) правила работы с ресурсами сети Интернет.

3. Требования к размещению серверного и коммуникационного оборудования ИКС

1. Серверы и коммуникационное оборудование образовательного учреждения располагаются только в выделенных помещениях.
2. Серверное и коммуникационное оборудование, обеспечивающее функционирование ИКС:
а) эксплуатируется и своевременно обслуживается в соответствии с инструкциями производителя;
б) должно быть надежно защищено от несанкционированного доступа к нему посторонних лиц.
3. Помещения, в которых установлено серверное и коммуникационное оборудование ИКС, оборудуются:
а) пожарно-охранной сигнализацией;
б) системой кондиционирования воздуха;
в) средствами пожаротушения.
4. Доступ в данные помещения ограничивается в соответствии со служебными обязанностями сотрудников. Перечень сотрудников, имеющих доступ в данные помещения, определяется руководителем образовательного учреждения.
5. Присутствие посторонних лиц в помещениях с оборудованием ИКС допускается только в сопровождении лиц, имеющих право доступа в данное помещение.
6. Ввод в эксплуатацию, установку и замену серверного и коммуникационного оборудования ИКС осуществляет инженер-электроник. Допускается привлекать, на основе дого-

вора, сторонних специалистов в присутствии ответственных за эксплуатацию оборудования.

4. Программное обеспечение ИКС

Установку и настройку ПО серверов и рабочих станций проводит инженер-электроник. Допускается привлекать, на основе договора, сторонних специалистов в присутствии ответственных за эксплуатацию оборудования.

5. Организация доступа в ИКС

1. Доступ к ресурсам ИКС предоставляется сотрудникам и студентам колледжа для исполнения их функциональных обязанностей.
2. Допускается предоставление временного ограниченного доступа к определенным информационным ресурсам ИКС лицам, не являющимся сотрудниками колледжа по согласованию с руководителем образовательного учреждения.
3. Все СВТ регистрируются в домене.
4. Регистрацию СВТ и пользователей в домене осуществляет инженер-электроник.
5. При регистрации в домене пользователям ИКС предоставляются персональные идентификационные данные - учетная запись и пароль.

6. Защита и хранение информации в ИКС

1. Основными целями защиты информации, обрабатываемой в ИКС, являются:

а) обеспечение защиты информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации;

б) соблюдение конфиденциальности информации.

2. Информация, собираемая, обрабатываемая и накапливаемая сотрудниками колледжа хранится на служебных компьютерах. Выделение ресурсов для хранения информации сотрудников колледжа осуществляет инженер-электроник.
3. Информация, накапливаемая на серверах и в информационных системах, подлежит обязательному резервному копированию.
4. Доступ к ресурсам сети Интернет и корпоративной электронной почте предоставляется через сервера образовательного учреждения. Подключение ИКС к сети Интернет и корпоративной электронной почте осуществляется с применением средств защиты, соответствующих требованиям законодательства Российской Федерации.
5. Инженер-электроник осуществляет контроль выполнения требований информационной безопасности.

Он вправе:

1) проводить проверки СВТ, подключенных к ИКС, с целью соблюдения требований информационной безопасности;

2) прекращать использование СВТ, подключенных к ИКС или применяемых для до-

ступа к информационным ресурсам ИКС, в случае выявления нарушений требований информационной безопасности;

3) вмешиваться в работу СВТ для предотвращения порчи, кражи и подмены информации;

4) инициировать проведение служебных расследований в случае выявления фактов нарушения требований информационной безопасности.

7. Ответственность

1. Ответственность за организацию надежного функционирования и организацию информационной безопасности ИКС несет заместитель директора по УПР.

2. Пользователи ИКС несут персональную ответственность за невыполнение требований настоящего Положения.

3. За нарушения в области компьютерных технологий, связанных с осуществлением несанкционированного доступа к информации, распространением вредоносных программ, нарушением работы ИКС, предусматривается ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1

ПРАВИЛА РАБОТЫ С РЕСУРСАМИ СЕТИ ИНТЕРНЕТ В ГБПОУ «ТКСиТ»

1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций.

2. При работе с сетью Интернет требуется соблюдение правил безопасности:

1) Старайтесь работать только с известными и проверенными ресурсами сети интернет, официальными сайтами разработчиков программного обеспечения.

2) Необходимо следить за адресами, на которые ведут ссылки. Для того чтобы узнать адрес, на который ведет ссылка необходимо просто навести на нее курсор.

3) Перед вводом личной информации проверяйте адресную строку браузера. Не сохраняйте пароли на чужих компьютерах. Злоумышленники используют поддельные сайты для кражи паролей и других важных данных. После получения доступа к вашему аккаунту злоумышленники могут использовать его для рассылки спама и вирусов.

4) Не переходите по незнакомым ссылкам, которые приходят вам на почту или в социальные сети. Даже если ссылка пришла от знакомого человека необходимо быть максимально внимательным. Вполне возможно аккаунт вашего знакомого уже взломан, и теперь от его имени рассылают вирусы.

5) Относитесь с подозрением к файлам, скаченным с непроверенных источников и файлообменников. Обязательно проверяйте их антивирусной программой.

6) Современные поисковые системы и браузеры, такие как Yandex, умеют предупреждать пользователя, когда он пытается зайти на сайт, распространяющий вирусы. Необходимо внимательно относиться к таким предупреждениям, скорее всего сайт, который вы пытаетесь посетить, заражен.

7) Не кликайте по подозрительным рекламным баннерам, предлагающим мгновенное обогащение или другие нереально выгодные услуги и сервисы. Скорее всего, вас пытаются обмануть.

3. Администрация ГБПОУ «ТКСиТ» оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей и учебному процессу:

1) ресурсы, содержание и направленность которых запрещены международным и федеральным законодательством;

2) материалы, носящие угрожающую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц;

3) материалы, способствующие разжиганию национальной розни, подстрекание к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и так далее;

4) материалы развлекательного характера.

4. При работе с ресурсами сети Интернет запрещено:

1) разглашение служебной информации, ставшей известной пользователю по служебной необходимости либо иным путем;

2) использовать в сети Интернет сайты, позволяющие работать анонимно, а также использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному политикой информационной безопасности;

3) использовать не лицензионное программное обеспечение, не сертифицированное на территории Российской Федерации, для доступа в сеть Интернет;

4) просматривать сайты порнографической, эротической, развлекательной направленности, и сайты, содержание которых не относится напрямую к исполнению служебных обязанностей сотрудников, играть в онлайн игры;

5) использовать программы для извлечения денежной выгоды в глобальной сети Интернет;

6) скачивать музыкальные и видео-файлы, запускать скаченные из сети Интернет исполняемые файлы без предварительной проверки на наличие вирусов, а также файлы, не имеющие отношения к текущим служебным обязанностям.

5. Не рекомендуется посещение ресурсов, транслирующих потоковое аудио и видео, создающих большую загрузку в сети, и мешающих нормальной работе остальных пользователей (веб-камеры, трансляция ТВ и музыкальных программ, радиовещательные Интернет станции).

6. Запрещено предоставлять доступ к сети Интернет в любой форме посторонним лицам, а также предоставлять доступ к информационным каналам сети пользователям других сетей используя специализированное ПО или оборудование.

7. При работе с Интернет-ресурсами, использующими авторизацию, владелец учетной

записи несет ответственность за соблюдение секретности пароля и действия, выполненные с использованием выданного идентификатора.

8. Доступ в сеть Интернет возможен только при установленном и работающем антивирусном программном обеспечении.

9. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой информационной безопасности.

Приложение № 2

ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ В ГБПОУ «ТКСиТ»

1. Электронная почта (имя@proftouoy.ru, tcsit@mail.ru, buhpl48@mail.ru, lizey48@mail.ru) является служебной почтой ГБПОУ «ТКСиТ» и может быть использована только в соответствующих целях. Использование электронной почты в других целях категорически запрещено. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями, предъявляемыми к оформлению официальных документов в электронном виде.

2. При работе с корпоративной системой электронной почты сотрудникам ГБПОУ «ТКСиТ» запрещается:

1) использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с инженером-электроником;

2) размещение своего корпоративного электронного адреса (имя@proftouoy.ru) либо адресов других сотрудников ГБПОУ «ТКСиТ» на общедоступных Интернет-ресурсах, если это не связано с исполнением служебных обязанностей, а также использовать для регистрации в сети Интернет (форумы, конференции, гостевая книга, доска объявлений, социальные сети и так далее);

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

4) осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия, если это только не связано со служебными обязанностями. Данные действия квалифицируются как Спам и являются незаконными;

5) рассылать 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;

6) рассылать через электронную почту 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;

7) фальсифицировать обратный адрес электронной почты, а также использовать иден-

тификационные данные (имена, адреса, телефоны и тому подобное) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование;

8) распространять защищенные авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

9) распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, порнографию, 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 так далее;

10) распространять информацию ограниченного доступа, содержащую конфиденциальные сведения или государственную тайну;

11) предоставлять другим пользователям пароль доступа к своему почтовому ящику.

3. Для получения доступа к корпоративной почте ГБПОУ «ТКСиТ» необходимо направить в адрес руководителя ГБПОУ «ТКСиТ» письмо с указанием Ф.И.О. и должности сотрудника.

Разработчики — Логинова Н.В., заместитель директора УР
Мамаев А.Д., инженер-электроник

Рассмотрено — Антипова А.В., заместитель директора по УВР
Кирьянова Т.О., главный бухгалтер
Шелуханова О.А., зав. отделением по специальностям