Государственное бюджетное профессиональное образовательное учреждение
«Сокольский техникум индустрии сервиса и предпринимательства»

ПРИКАЗ

«31» марта 2017г. № 56

Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным крутом лиц

В целях обеспечения необходимого уровня информационной безопасности в Государственном бюджетном профессиональном образовательном учреждении «Сокольский техникум индустрии сервиса и предпринимательства» (далее -ГБПОУ СТИСП) приказываю:

1. Утвердить Положение по обеспечению информационной безопасности при использовании в ГБПОУ СТИСП информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным крутом лиц» согласно приложения.
2. Разместить настоящий приказ на официальном сайте учреждения в течение десяти рабочих дней со дня издания настоящего приказа.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор  Подколзина Н. А.

Приложение
к приказу ГБПОУ СТИСП
№ 56 от «31» марта 2017 г.

ПОЛОЖЕНИЕ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «СОКОЛЬСКИЙ ТЕХНИКУМ ИНДУСТРИИ СЕРВИСА И ПРЕДПРИНИМАТЕЛЬСТВА» ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ДОСТУП К КОТОРЫМ НЕ ОГРАНИЧЕН ОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ

I. Общие положения

1.1. Настоящее Положение определяет условия и порядок предоставления доступа и использования в ГБПОУ «Сокольский техникум индустрии сервиса и предпринимательства» (далее- ГБПОУ СТИСП) информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, и позволяющих обрабатывать информацию с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), и их ресурсов, правила работы в сети "Интернет", угрозы безопасности информации и меры обеспечения безопасности информации при использовании сети "Интернет", порядок предоставления доступа и использования электронной почты, права, обязанности и ответственность их сотрудников (далее - пользователи) в рамках настоящего Положения.

1.2. Настоящее Положение разработано на основе:

Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года № 646;

Указа Президента Российской Федерации от 22 мая 2015 года № 260 "О некоторых вопросах информационной безопасности Российской Федерации";

Указа Президента Российской Федерации от 17 марта 2008 года № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

Концепции информационной безопасности Нижегородской области, утвержденной постановлением Правительства Нижегородской области от 31

декабря 2015 года № 920.

Распоряжения Правительства Нижегородской области от 17.02.2017 № 151-р "Об утверждении Положения по обеспечению информационной безопасности при использовании в органах исполнительной власти Нижегородской области информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц"

1.3. В настоящем Положении применяются понятия, установленные действующим законодательством Российской Федерации в области информации, информационных технологий и защиты информации, а также следующие понятия, определения и сокращения:

"КСПД" - корпоративная сеть передачи данных, функционирующая в соответствии с постановлением Правительства Нижегородской области от 29 августа 2008 года № 365 "О корпоративной сети передачи данных";

"АРМ" - выделенное автоматизированное рабочее место имеющее доступ к сети "Интернет";

"ресурс" - информационная система и информационный ресурс;

"локальная сеть" - локальная информационно-телекоммуникационная (вычислительная) сеть.

II. Цели использования сети "Интернет"

Основными целями использования сети "Интернет" в ГБПОУ СТИСП являются:

1) обеспечение в соответствии с Федеральным законом от 9 февраля 2009 года № 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", постановлением Правительства Российской Федерации от 10 июля 2013 года № 583 "Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети "Интернет" в форме открытых данных", постановлением Правительства Нижегородской области от 14 июля 2010 года № 422 "Об обеспечении доступа к информации о деятельности Губернатора Нижегородской области, Правительства Нижегородской области, органов исполнительной власти Нижегородской области" реализации функций и полномочий, в том числе свободного доступа к информации о деятельности ГБПОУ СТИСП с применением информационных технологий;

2) размещение ГБПОУ СТИСП достоверной и своевременно обновленной информации о деятельности в сети "Интернет";

3) поиск и получение информации в сети "Интернет", необходимой для выполнения должностных обязанностей пользователей;

4) осуществление закупок товаров, работ, услуг для обеспечения нужд ГБПОУ СТИСП ;

5) обеспечение функционирования информационных систем требующих для их корректной работы наличие подключения к сети "Интернет";

6) обеспечение в служебных целях доступа (взаимодействия) к сторонним информационным системам и их сервисам, работающим с использованием сети "Интернет";

7) передача (получение) информации в (из) сеть "Интернет" в рамках исполнения должностных обязанностей пользователей;

8) обеспечение информационного взаимодействия внутри ГБПОУ СТИСП между собой и с иными организациями, в том числе посредством электронной почты.

III. Угрозы безопасности информации при использовании сети "Интернет"

3.1. Использование сети "Интернет" в ГБПОУ СТИСП создает риски:

1) заражения АРМ программными вирусами;

2) несанкционированного доступа к информационно-вычислительным ресурсам и системам ГБПОУ СТИСП (в том числе целенаправленные сетевые атаки);

3) внедрения в информационные системы ГБПОУ СТИСП программных закладок;

4) загрузки трафика нежелательной корреспонденцией, массовыми, незапрашиваемыми рекламными сообщениями или коммерческими предложениями (спамом);

5) несанкционированной передачи информации ограниченного доступа в сеть "Интернет";

6) нарушения доступности информационно-вычислительных ресурсов в ГБПОУ СТИСП;

7) нарушения целостности и достоверности открытых, и общедоступных ресурсов ГБПОУ СТИСП размещаемых им в сети "Интернет" по требованиям действующего законодательства;

8) нарушения конфиденциальности, целостности и доступности информации ограниченного доступа, передаваемой по сети "Интернет".

3.2. Основными группами потенциальных угроз безопасности информации при использовании сети "Интернет"в ГБПОУ СТИСП ведущими к реализации рисков, являются:

1) угрозы утечки информации по техническим каналам;

2) угрозы использования штатных средств информационных систем с целью совершения несанкционированного доступа к информации;

3) угрозы нарушения доступности информации;

4) угрозы нарушения целостности информации;

5) угрозы нарушения конфиденциальности информации;

6) угрозы недекларированных возможностей в системном и прикладном программном обеспечении;

7) угрозы, не являющиеся атаками;

8) угрозы несанкционированного доступа, создающие предпосылки для реализации такого доступа в результате нарушения процедуры авторизации и аутентификации;

9) угрозы несанкционированного доступа к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

10) угрозы ошибок или внесения уязвимостей при проектировании, внедрении информационных систем и их систем защиты;

11) угрозы ошибочных или деструктивных действий лиц;

12) угрозы программно-математических воздействий;

13) угрозы, связанные с использованием облачных услуг;

14) угрозы, связанные с использованием технологий виртуализации;

15) угрозы, связанные с нарушением правил эксплуатации машинных носителей;

16) угрозы, связанные с нарушением процедур установки и обновления программного обеспечения и оборудования;

17) угрозы физического доступа к компонентам информационных систем;

18) угрозы эксплуатации уязвимостей в системном и прикладном программном обеспечении, средствах защиты информации, аппаратных компонентах информационных систем, микропрограммном обеспечении;

19) угрозы, связанные с использованием сетевых технологий;

20) угрозы инженерной инфраструктуры;

21) угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

22) угрозы, связанные с контролем защищенности информационной системы;

23) угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

IV. Меры обеспечения безопасности информации при использовании сети "Интернет"

Основными мерами по предотвращению реализации рисков и угроз, указанных в разделе III настоящего Положения, являются:

1) создание автоматизированной системы доступа к ресурсам сети "Интернет" (далее - АСД), представляющей собой комплекс программно-технических мер, предназначенных для организации стабильного гарантированного и безопасного доступа к ресурсам сети "Интернет";

2) использование в соответствии с выявленными актуальными угрозами безопасности информации актуальных версий средств защиты информации (средств межсетевого экранирования, средств контроля и анализа данных, передаваемых по сети "Интернет", средств анализа защищенности, средств защиты от несанкционированного доступа, средств антивирусной защиты, средств криптографической защиты информации, средств детектирования (предотвращения) вторжений (атак) из сети "Интернет" и вредоносного программного обеспечения, и т.п.), прошедших сертификацию в Федеральной службе безопасности Российской Федерации

(далее - ФСБ России) и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России);

3) запрет доступа к потенциально опасным и деструктивным Интернет-сервисам и ресурсам в сети "Интернет", Интернет-сервисам, серверное оборудование которых располагается за пределами Российской Федерации, в том числе к сетевым хранилищам и облачным технологиям, функционирующим за пределами Российской Федерации;

4) использование КСПД;

5) учет программных и технических средств для доступа к ресурсам сети "Интернет";

6) проведение при необходимости аттестационных испытаний;

7) определение актуальных угроз и возможных нарушителей безопасности информации;

8) разработка необходимой документации по обеспечению информационной безопасности;

9) определение организационных и технических мер по обеспечению информационной безопасности;

10) контроль и анализ информации, передаваемой с использованием сети "Интернет";

11) анализ сведений о работе с ресурсами сети "Интернет";

12) проведение мероприятий по оценке защищенности доступа в сеть "Интернет".

V. Условия и порядок доступа к ресурсам сети "Интернет"

5.1. Доступ к сети "Интернет" предоставляется пользователю только в целях, указанных в разделе II настоящего Положения, исходя из принципа предоставления минимально необходимых привилегий в целях исполнения им должностных обязанностей. Иное использование ресурсов сети "Интернет", решение о котором не принято в установленном порядке, должно рассматриваться как нарушение политики информационной безопасности.

5.2. Доступ пользователя к ресурсам сети "Интернет" осуществляется с закрепленного за ним АРМ, входящего в АСД. Пользователю запрещается использовать АРМ, не входящие в АСД, для доступа к сети "Интернет".

5.3. Предоставление (блокирование) доступа пользователю к определенным ресурсам сети "Интернет" осуществляется с помощью программных средств по решению его руководителя, принимаемому по представлению Администратора АСД, которое содержит перечень ресурсов сети "Интернет", доступ к которым необходимо обеспечить или заблокировать, список пользователей и цели предоставления (блокирования) доступа.

VI. Правила использования электронной почты

Пользователю запрещается:

1) передавать информацию, не относящуюся к служебной деятельности;

2) передавать информацию, носящую клеветнический или непристойный характер, а также содержащую угрозы, оскорбляющую честь и достоинство других лиц, порочащую деловую репутацию, материалы, способствующие разжиганию межнациональной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, коррупции и т.д.;

3) передавать логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет;

4) через личные электронные почтовые адреса, передавать электронные почтовые сообщения, содержащие служебную информацию/информацию ограниченного доступа;

5) использовать электронные почтовые адреса, для оформления подписки на периодическую почтовую рассылку материалов из сети Интернет, а также для регистрации на интернет-ресурсах, не связанных с исполнением должностных обязанностей;

6) предоставлять доступ к электронному почтовому адресу либо сообщать пароль доступа к нему лицам, не уполномоченным на обладание такими сведениями;

7) переходить по ссылкам и открывать вложенные файлы входящих электронных почтовых сообщений, полученных от неизвестных отправителей;

8) осуществлять с электронных почтовых адресов, рассылку (в том числе массовую) электронных почтовых сообщений, в том числе рекламного характера, если это не связано с исполнением должностных обязанностей;

VII. Правила работы в сети "Интернет"

7.1. При получении пользователем доступа к сети "Интернет" с АРМ ему запрещается:

1) заходить на ресурсы сети "Интернет", компрометирующие его как пользователя;

2) использовать ресурсы сети "Интернет" и программное обеспечение для доступа в сеть "Интернет", являющиеся потенциально опасными и деструктивными, и создающие угрозу безопасности информации (ее предпосылки);

3) использовать Интернет-сервисы и ресурсы сети "Интернет", не связанные со служебной (трудовой) деятельностью пользователя;

4) использовать для передачи (обработки) информации ограниченного доступа Интернет-сервисы, Интернет-пейджеры (программы для мгновенного обмена сообщениями через сеть "Интернет" в режиме реального времени) и файлообменники, не обеспечивающие конфиденциальность

передаваемой информации;

5) скачивать, устанавливать и обновлять на АРМ любое программное обеспечение;

6) изменять состав и конфигурацию программных и технических средств АРМ;

7) работать на АРМ под чужой учетной записью / не персонифицированной учетной записью;

8) использовать доступ к сети "Интернет" для совершения попыток на получение доступа к закрытым ресурсам, для распространения и тиражирования информации, направленной на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за незаконное распространение которой предусмотрена уголовная или административная ответственность;

9) использовать сетевые хранилища и облачные технологии, функционирующие за пределами Российской Федерации, для обработки и хранения данных (конфиденциальных, ограниченного доступа, служебных).

7.2. Пользователю запрещается самостоятельно создавать, устанавливать и использовать беспроводные сети доступа к сети "Интернет", взаимодействующие на физическом уровне с АРМ, используемыми в АСД.

7.3. Пользователь использует только Интернет-браузеры, которые разрешены к использованию Администратором АСД.

7.4. При работе с информационными системами, локальными сетями, средствами вычислительной техники, в том числе АРМ, имеющими подключение к сети "Интернет", Администратору АСД и пользователю необходимо руководствоваться следующей парольной политикой:

1) организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, и контроль за действиями пользователей при работе с паролями возлагается на Администратора АСД;

2) пароли доступа к АРМ первоначально формируются Администратором АСД, а в дальнейшем выбираются пользователями самостоятельно, но с учетом следующих требований: длина пароля должна быть не менее 8 символов; в числе символов пароля должны присутствовать прописные буквы латинского алфавита от A до Z, строчные буквы латинского алфавита от a до z, десятичные цифры (от 0 до 10), неалфавитные символы (@, #, $, &, *, % и т.п.). Исключение составляют АРМ, в которых использование подобных спецсимволов недопустимо; пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.); при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами;

3) пользователь несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных (легкодоступных) местах;

4) в случае производственной необходимости (командировка, отпуск и

т.п.), при проведении работ, требующих знания пароля пользователя, допускается раскрытие значений своего пароля Администратору АСД. По окончании производственных или проверочных работ пользователи самостоятельно производят немедленную смену значений "раскрытых" паролей;

5) в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей пользователей (в их отсутствие) допускается изменение паролей Администратором АСД. В подобных случаях пользователи, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей создать их новые значения;

6) полная плановая смена паролей пользователей должна проводиться в срок не позднее 90 дней после установления предыдущего пароля. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к Администратору АСД;

7) внеплановая смена личного пароля или удаление учетной записи пользователя АРМ или информационной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться Администратором АСД в течение 1 рабочего дня после окончания последнего сеанса работы данного пользователя с АРМ или информационной системой;

8) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение) Администратора АСД и других пользователей, которым по роду работы были предоставлены полномочия по управлению парольной защитой (политикой);

9) в случае компрометации личного пароля пользователя АРМ либо подозрении на компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием Администратора АСД;

10) смена забытого пользовательского пароля производится Администратором АСД на основании сообщения пользователя с обязательной установкой параметра "Требовать смену пароля при следующем входе в систему";

VIII. Размещение (публикация) в сети "Интернет" информации

Пользователь размещает (публикует) в сети "Интернет" информацию, не запрещенную к размещению (публикации) действующим законодательством.

IX. Контроль работы пользователей с сетью "Интернет"

9.1. Для контроля работы пользователей с ресурсами сети "Интернет"

проводятся организационные и технические мероприятия, в том числе применяются средства контроля доступа пользователей к ресурсам (сайтам) сети "Интернет" (далее - СКД).

9.2. Функционирование СКД должно осуществляться в соответствии со следующей политикой информационной безопасности:

1) для распределения политик доступа различных категорий пользователей к определенным ресурсам сети "Интернет" в АСД следует создавать соответствующие группы в настройках СКД;

2) за использование учетной записи кем-либо, кроме пользователя, которому она была присвоена и выдана, пользователь несет персональную ответственность;

3) пользователь несет персональную ответственность за сохранность в тайне своего персонального пароля. Сохранение пароля пользователя в Интернет-браузере (программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой), фиксация пароля на общедоступных носителях информации (стикерах, записках, в текстовых файлах и т.д.), а также разглашение пароля неуполномоченным третьим лицам запрещены;

4) разрешается использовать лишь те ресурсы (сайты) сети "Интернет", которые необходимы для выполнения должностных обязанностей.

9.3. По мере накопления статистических данных об использовании ресурсов сети "Интернет" политика безопасности СКД может быть дополнена Администратором АСД.

X. Права, обязанности и ответственность

10.1. Администратор АСД:

1) обеспечивает функционирование и осуществляет контроль эксплуатации АСД;

2) блокирует при помощи СКД доступ пользователей ГБПОУ СТИСП к ресурсам сети "Интернет", используемым пользователем не в целях, указанных в разделе II настоящего Положения, и к ресурсам сети "Интернет" из Списка;

3) обеспечивает в рамках своей компетенции безопасный доступ к ресурсам сети "Интернет";

4) принимает меры по недопущению подключения к потенциально опасным и деструктивным Интернет-сервисам и ресурсам в сети "Интернет", Интернет-сервисам, серверное оборудование которых располагается за пределами Российской Федерации, в том числе к сетевым хранилищам и облачным технологиям, функционирующим за пределами Российской Федерации;

5) устанавливает, обновляет и настраивает для работы пользователей Интернет-браузеры, в том числе российские Интернет-браузеры, поддерживающие установку защищенных соединений как с односторонней, так и с двухсторонней аутентификацией, с использованием российских

криптографических алгоритмов, имеющие в составе сервисные функции, предназначенные для предотвращения атак на пользователя Интернет-браузера, организованных с помощью фишинга, вредоносных (мошеннических) сайтов и перехвата личных данных, а также автоматически проверяющие загружаемые файлы с помощью антивирусных технологий, за исключением случаев, когда выполнение должностных обязанностей пользователя с использованием российского Интернет-браузера невозможно;

6) осуществляет управление обновлениями вирусных баз антивирусного программного обеспечения: устанавливает автоматический режим ежедневного обновления вирусных баз на всех АРМ, имеющих подключение к сети "Интернет";

7) реагирует на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения посредством сети "Интернет";

8) в целях защиты общедоступной информации, размещаемой в сети "Интернет", использует средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получившие подтверждение соответствия в ФСТЭК России;

9) при необходимости может устанавливать дополнительные правила работы в сети "Интернет" для пользователей, не противоречащие требованиям действующего законодательства.

10.2. Пользователь несет персональную ответственность за несоблюдение запретов и ограничений, установленных настоящим Положением.

Принято
на заседании Совета Техникума
Протокол от «31» марта 2017г.