**ПРИНЯТО**

**Решением Совета Учреждения**

**От «17» апреля 2020 г.**

**Протокол № 9**

**Утверждено**

**приказом директора техникума №70**

**от «17» апреля 2020 г.**

**Положение**
**об информационной безопасности областного государственного бюджетного профессионального образовательного учреждения «Спасский политехнический техникум»**

**1. Общие положения**

1.1. Настоящее Положение об информационной безопасности является нормативным локальным актом ОГБПОУ «Спасский политехникум» (далее – Учреждение) и обязательно к исполнению всеми участниками образовательных отношений.

1.2. Настоящее Положение подготовлено на основе:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации»;
- Трудового кодекса Российской Федерации;
- Федерального закона от 29.12.2010 № 436-ФЗ ( в ред. от 28.07.2012 ) «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. В Учреждении развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локально-вычислительной сети Учреждения понимается ёе защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

Безопасность системы обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности, связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

Систему обеспечения безопасности включает следующие подсистемы:

— компьютерную безопасность;
— безопасность данных;
— безопасное программное обеспечение;
— безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

1.4. К объектам информационной безопасности Учреждения относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации - средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.5. Ответственные за информационную безопасность назначаются приказом директора Учреждения и подчиняются директору Учреждения.

1.6. Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

1.7. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств Учреждения.

1.8. В случае кадровых перестановок и изменений все ответственные за базы данных переназначаются приказом директора Учреждения, новым сотрудникам предоставляются логины и пароли для доступа к базам данных.

## 2. Основные задачи и функции ответственных за информационную безопасность

2.1. Основными задачами ответственных за информационную безопасность являются:

- организация эксплуатации технических и программных средств защиты информации;
- текущий контроль работы средств и систем защиты информации;
- организация и контроль резервного копирования информации на сервере ЛВС.

2.2 Ответственные за информационную безопасность выполняют следующие основные функции:

- разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
- обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.
- организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Учреждение;
- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
- контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
- контроль пользования Интернетом.

## 3. Права ответственных лиц за информационную безопасность

3.1. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

3.2. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

**4. Обязанности ответственных лиц за информационную безопасность**

4.1. Обеспечение функционирования и поддержания работоспособности средств и систем защиты информации, в пределах, возложенных на них обязанностей.

4.2. Немедленное информирование директора Учреждения о выявленных нарушениях и несанкционированных действиях пользователей, в том числе о случаях несанкционированного доступа в Интернет, а также принятие необходимых мер по устранению нарушений.

4.3. Принятие мер по восстановлению работоспособности средств и систем защиты информации.

4.4. Проведение инструктажей сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

4.5. Создание и удаление учетных записей пользователей.

4.6. Администрирование работы сервера ЛВС, размещение и классифицирование информации на сервере ЛВС.

4.7. Установление по согласованию с директором Учреждения критериев доступа пользователей на сервер ЛВС.

4.8. Формирование и представление паролей для новых пользователей, администрирование прав пользователей.

4.9. Отслеживание работы антивирусных программ, проведение один раз в неделю полной проверки компьютеров на наличие вирусов.

4.10. Регулярное выполнение резервного копирования данных на сервере, при необходимости восстановление потерянных или поврежденных данных.

4.11. Ежемесячная подача директору Учреждения статистической информации по пользованию Интернетом.

4.12. Ведение и учет пользователей «точки доступа к Интернету». В случае необходимости, лимитирование времени работы пользователя в Интернете и объема скачиваемой информации.

**5. Ответственность ответственных лиц за информационную безопасность**

5.1. На ответственных за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.

**6. Система аутентификации**

6.1. На клиентских ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 10.

6.2. Для использования локальной вычислительной сети в учебном процессе используются групповая идентификация: пользователь - обучающийся, пользователь преподаватель, администратор с разграничением прав доступа к папкам файлового сервера.

6.3. Для всех пользователей баз данных устанавливаются уникальные пароли.

6.4. Периодичность плановой смены паролей 1 раз в начале учебного года.

6.5. Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз.

6.6. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 15 мин., с последующим вводом пароля для разблокирования ПК.

6.7. Обязать пользователей осуществлять выход из базы данных, если планируется отсутствие на рабочем месте более 1,5 часов.

6.8.. Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

## 7. Антивирусная защита

7.1. Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

7.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

7.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.

Приложение 1

**Рекомендации для родителей «Безопасный интернет»**

Уважаемые родители! Если ваши дети пользуются Интернетом, вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать в путешествии по этому океану информации. Значительное распространение материалов, предназначенных только для взрослых или неприемлемых для детей по какой-либо другой причине, может легко привести к неприятным последствиям. Кроме того, в Сети нередко встречаются люди, которые пытаются с помощью Интернета вступать в контакт с детьми, преследуя опасные для ребенка или противоправные цели.

Основные правила для родителей

1. Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить вас пользоваться различными приложениями, которыми вы не пользовались ранее.

2. Помогите своим детям понять, что они не должны размещать в Сети информацию о себе: номер мобильного телефона, домашний адрес, а также показывать фотографии (свои и семьи). Ведь любой человек может это увидеть и использовать в своих интересах.

3. Если ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в таких письмах и ни в коем случае не отвечал на них.

4. Объясните детям, что нельзя открывать файлы, присланные незнакомыми людьми. Эти файлы могут содержать вирусы или фото-, видеоматериалы непристойного или агрессивного содержания.

5. Объясните, что некоторые люди в Интернете могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны самостоятельно, без взрослых встречаться с сетевыми друзьями, которых не знают в реальной жизни.

6. Постоянно общайтесь со своими детьми, рассказывайте, советуйте, как правильно поступать и реагировать на действия других людей в Интернете.

7. Научите своих детей правильно реагировать, если их кто-то обидел в Сети или они получили / натолкнулись на агрессивный контент. Расскажите, куда в подобном случае они могут обратиться.

8. Убедитесь, что на компьютере, которым пользуются ваши дети, установлены и правильно настроены средства фильтрации. Помните! Эти простые меры, а также доверительные беседы с детьми о правилах работы в Интернете позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное путешествие по Всемирной сети.

Приложение 2

**Рекомендации для сотрудников Учреждения**

1 .Если раньше взрослые старались предостеречь детей от опасностей, которые подстерегают их на улице, то сегодня возникла проблема безопасности ребёнка в киберпространстве. Для того чтобы обеспечить эту безопасность необходимо в первую очередь самим хорошо знать эту зону. В рамках данного исследования самими педагогами не раз поднималась проблема того, что их уровень знаний информационного пространства значительно отстает от знаний детей. Поэтому в первую очередь необходимо повышать уровень информационной грамотности самих педагогов.

2. Преподавателям в рамках своих уроков необходимо как можно больше применять современных информационных технологий и сразу предостерегать своих студентов о возможном их негативном влиянии.

3. В воспитательной работе уделять внимание воспитанию информационной культуры обучающихся.

4. Проводить уроки медиаобразования, на которых давать самые необходимые знания по соблюдению безопасности в информационном пространстве.

5. Многие рекомендации, которые уже были даны в разделе Рекомендации для родителей, могут пригодиться и специалистам, работающим со студентами.

6. Каждый пользователь при работе в Интернете сталкивается с нежелательным контентом. Речь идет не только о той информации, которую пользователь не хотел получать. Нежелательным контентом являются: вирусы, трояны и прочие вредоносные объекты; фишинг, перехват паролей; сетевые атаки; утечка важной информации; киберпреследование и злоупотребление персональными данными.

Кроме того, существует определенная информация, доступ к которой необходимо ограничить, например, если за компьютером находится подросток. Решением всех этих проблем является использование системы контетной фильтрации.

Похожей системой пользуются антивирусы и фаерволлы, защищающие компьютер от вирусов и сетевых атак. Фильтрация сайтов осуществляется с помощью любого браузера или Интернет-фильтра. Они контролируют поток Интернет-трафика через определение категории сайта по его содержимому. Это особенно актуально для ресурсов, которые содержат информацию разных категорий. Дело осложняется тем, что технологии не стоят на месте. Сайты создаются с помощью новых инструментов, а это требует разработки новых технологий фильтрации Интернет-трафика. Что касается программного обеспечения, которое помогает осуществлять контентную фильтрацию, то их существует очень много. Они представлены в виде комплексных контент-фильтров и маленьких плагинов для Интернет-браузеров. Особенно богат выбор среди средств защиты детей от Интернет-угроз. С помощью современного ПО можно ограничить детям доступ в Интернет, блокировать взрослый контент, следить на какие страницы он заходит и сколько времени проводит в Сети. С помощью стандартного контент-фильтра можно:

- регулировать время прибывания в Интернете;
- регулировать доступ на определенные сайты;
- запрещать посещение сайтов с определенным контентом;
- отключить загрузку флеш-рекламы;
- отключить всплывающие окна;
- запрещать автоматические переходы на другие сайты

7. Проблема информационной безопасности образовательного учреждения превращается во вполне реальную. Количество угроз растет с каждым днем, изменяется нормативно-правовая база, соответственно реалиям времени должны изменяться и методы обеспечения информационной безопасности учебного процесса. В образовательной организации информация, информационная инфраструктура - один из главных компонентов учебного процесса. Учебные кабинеты оснащены компьютерной техникой, и её качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию профессиональных компетенций обучающихся. Поэтому обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важной для его качества.

Приложение 3

**Рекомендации обучающимся Учреждения по организации работы в информационном пространстве**

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.

2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.

3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве

4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.

5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.

6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.

7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные вебсайты. Для интернет-преступников вы становитесь лёгкой добычей.

8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.

9. Не используйте в логине или пароле персональные данные. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.

10. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.

11. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.

12. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.

13. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.

14. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.

15. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.

16. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан «Сегодня реальная жизнь, как взрослых, так и детей, все больше уходит в виртуальное пространство. Однако следует понимать, что Интернет — это не только здорово, но и опасно.