Областное государственное бюджетное профессиональное образовательное учреждение
«Рязанский политехнический колледж»

ОДОБРЕНО
На Совете колледжа
Протокол № 2
От «14» апреля 2020г.

УТВЕРЖДАЮ
Директор ОГБПОУ
«Рязанский политехнический колледж»
_____А.Ф.Смыслов
«_____»_____2020г.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Общие положения

1.1. Настоящее Положение об информационной безопасности (далее - Положение) Областного государственного бюджетного профессионального образовательного
учреждения «Рязанский политехнический колледж») разработано в соответствии:
- Ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации».
- Ст. 9 Закона № 149-ФЗ, п. 5 - информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей подлежит защите в случаях, предусмотренных законом (государственная тайна).
- Гл. 14 Трудового кодекса РФ (далее - ТК РФ) - защита персональных данных работника.
- Федеральным законом от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".
- Федеральным законом от 27.07.2006 № 152-ФЗ РФ «О персональных данных», обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

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

Под безопасностью локально-вычислительная сети Колледжа понимается ее 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.

К объектам информационной безопасности Колледжа относят:

— информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

— средства и системы информатизации

— средства вычислительной 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.

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность Колледжа.

1.3. Ответственные за информационную безопасность назначаются приказом директора Колледжа.

1.4. Ответственные за информационную безопасность подчиняются директору Колледжа.

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

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

2. Основные задачи и функции ответственных за информационную безопасность

2.1. Основными задачами ответственных за информационную безопасность являются:
2.1.1. Организация эксплуатации технических и программных средств защиты информации.
2.1.2. Текущий контроль работы средств и систем защиты информации.
2.1.3. Организация и контроль резервного копирования информации на сервере ЛВС.
2.2 Ответственные за информационную безопасность выполняют следующие основные функции:
2.2.1. Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
2.2.2. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.
2.2.3. Организация антивирусного контроля носителей информации и файлов электронной почты, поступающих в Колледж.
2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
2.2.5. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
2.2.7. 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 Колледжа 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 совместно с отделом ИТ по восстановлению работоспособности средств и систем защиты информации.
4.4. Проведение инструктажей сотрудников и пользователей ПК по правилам работы 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 Колледжа 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 полной проверки компьютеров на наличие вирусов осуществляется согласно регламенту.
4.10. Регулярное выполнение резервного копирования данных на сервере, при необходимости восстановление потерянных или поврежденных данных.
4.11. Ежемесячная подача директору Колледжа статистической информации по пользованию Интернетом.

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. Базы данных

6.1. Базы данных подлежащие защите вносятся в «Реестр баз данных подлежащих информационной защите».
6.2. Для каждой базы данных включенной в «Реестр баз данных подлежащих информационной защите» приказом директора Колледжа по представлению Комиссии по информационной безопасности назначается Ответственный за ведение базы данных.
6.3. Все процедуры по использованию и обслуживанию базы данных осуществляет ответственный за ведение базы данных. В том числе:

— резервное копирование;
— периодический контроль исправности резервных копий;
— подключение и отключение пользователей;
— внесение изменений в структуру базы, а также изменений в «Реестр баз данных подлежащих Информационной защите», при необходимости (изменение степени конфиденциальности, места расположения и т.д.);
— прочие виды работ, связанных с данной базой.

6.4. Все изменения «Реестра баз данных подлежащих информационной защите» осуществляется по решению Комиссии по информационной безопасности, состоящей из директора Колледжа, ответственного за информационную безопасность, ответственного за ведение базы данных.

6.6. В случае если база данных требует парольной защиты, то ответственный за базу данных руководствуется требованиями раздела «Система аутентификации» настоящего Положения.

7. Система аутентификации

7.1. На клиентских ПК используется WINDOWS XP, WINDOWS 10.
7.2. Для использования локальной вычислительной сети в учебном процессе используются групповая идентификация: пользователь - обучающийся, пользователь преподаватель, администратор с разграничением прав доступа к папкай файлового сервера.
7.3. Для всех пользователей баз данных устанавливаются уникальные пароли.
7.4. Периодичность плановой смены паролей 1 раз в начале учебного года.
7.5. Установить блокировку учетной записи пользователей при неправильном наборе пароля.
7.6. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 30 мин., с последующим вводом пароля для разблокирования ПК.
7.7. Обязать пользователей осуществлять выход из базы данных, если планируется отсутствие на рабочем месте более 1,5 часов.
7.8. Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.
7.9. Обслуживание системы аутентификации осуществляют ответственные за базы данных.

8. Защита по внешним цифровым линиям связи

8.1. В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю сеть (Интернет, электронная почта) осуществляется через компьютеры с установленными брандмауэром и антивирусом.

8.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.
8.3. Подключение рабочих станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet.

9. Защита от несанкционированного подключения к ЛВС и размещение активного сетевого оборудования

9.1. Колледжные серверы размещаются в специально оборудованных помещениях.
9.2. Доступ к серверам ограничен физически, программно и доступен системному администратору. за информатизацию, инженеру - программисту.
9.3. Коммутаторы, концентраторы, роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

10. Процедура увольнения сотрудников, имеющих доступ к сети

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

11. Антивирусная защита

11.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). 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.
11.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.
11.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.

ПРИЛОЖЕНИЕ 1.

ПАМЯТКА 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.

Меры предосторожности:

Побеседуйте с детьми. Первое, что необходимо объяснить: нахождение в Интернете во многом напоминает пребывание в общественном месте. Значительная часть опасностей, подстерегающих пользователя, очень схожи с риском, возникающим при общении с чужими людьми. Дети должны четко понимать: если они лично не знают человека, с которым общаются в Сети, это равносильно общению с незнакомцем в реальной жизни, что запрещено.

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
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. 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.

7. 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 специалистов учебного заведения.

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.

Памятка по безопасному использованию Интернета.

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.
Приняты меры по созданию безопасной информационной системы в колледже
• Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)
• Установлен контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией
• Установлены пароли на персональные ЭВМ

• Использованы контент-фильтры, для фильтрации сайтов по их содержимому. 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

ПРИЛОЖЕНИЕ 3.

Рекомендации студентам 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 веб сайты. 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.
10. 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.
11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.
12. 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.
13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.
14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.
15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.
16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.
17. 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.

Чтобы опыт в Сети был не только полезным, но и максимально позитивным, на странице портала http://www.edu22.info/projects/203-dlya-roditelej.html для родителей собрана самая полезная информация о безопасности в Интернете (по материалам краевой родительской академии «Интернет: возможности и опасности. Как защитить семью и ребенка?»).