государственное бюджетное профессиональное образовательное учреждение
Октябрьский коммунально- строительный колледж

УТВЕРЖДАЮ:

Директор ГБПОУ
Октябрьский
коммунально-строительный
колледж

_____Р.Р.Мардамшин

«01 » сентября 2014г

ПОЛИТИКА

информационной безопасности ГБПОУ Октябрьский коммунально -строительный колледж

1. Информационная безопасность

1.1 Общие положения

Информационной безопасностью определяются меры по защите информации от неавторизованного доступа, разрешения, модификации, раскрытия и задержек в доступе.

Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность дает гарантию того, что достигаются следующие цели:

- конфиденциальность критической информации
- целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода)
- доступность информации, когда она нужна
- учет всех процессов, связанных с информацией

• Следить за сроком действия ключей криптозащиты.

Существует два вида угроз информационной безопасности:

-внешняя - несанкционированный доступ из сети Интернет; снятие информации с кабельных систем (ЛВС и электропитания) при помощи технических средств; запись разговоров на расстоянии сквозь стены (окна, двери) и т. д.;

-внутренняя несанкционированный доступ в помещение; несанкционированный и неизбирательный доступ к данным внутри корпоративной сети; возможность записи информации на переносные устройства (флэш-накопители, CD- и DVD-диски и т.п.), пересылка фотоснимков бумажных носителей и экранов мониторов с помощью мобильных телефонов: программные вирусы и «троянские» программы.

1.2 Объекты информационной безопасности

Информационная система ОКСК, является организационно технической системой, в которой реализуются информационные технологии. и предусматривается использование аппаратного, программного и других видов обеспечения, необходимого для реализации информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации.

Основными элементами, составляющими такую систему, являются:

1. Локальные сети в учебных классах и подразделениях:
2. Рабочие места сотрудников ОКСК и студентов;
3. Носители информации (флеш, оптические и др.);
4. Информационные ресурсы.

Информационные ресурсы техникума включают в себя документальные и информационные потоки для обеспечения учебного процесса и хозяйственной деятельности техникума.

К ним относятся рабочие планы специальностей, рабочие программы дисциплин, учебные графики, сведения о контингенте . приказы и распоряжения директора, электронный каталог библиотеки,

электронные журналы и другие полнотекстовые базы данных, как создаваемые на месте, так и приобретаемые.

Информационные ресурсы классифицируются в ОКСК по следующим признакам:

- Общедоступная
- Ограниченного доступа

Под общедоступной информацией понимается информация собираемая, создаваемая и/или сохраняемая техникумом, которая не составляет государственную или иного вида тайну, определенную законодательством, либо уставом техникума. К ней можно отнести: учебные расписания. методички и др.

К информации ограниченного доступа относится информация. определенная законодательством или уставом техникума, как информация ограниченного доступа.

К данному типу можно отнести:

-Профессиональные секреты - секреты, связанные с организацией учебных процессов и др.;

-Персональные данные - под персональными данными понимается любая документированная и/или занесенная на машинные носители информация. которая относится к конкретному человеку и или которая может быть отождествлена с конкретным человеком.

-Документы по основной и финансово- хозяйственной деятельности. Отчеты в вышестоящие организации.

-Внутренние организационно-распорядительные документы.

1.3 Доступ и ответственность

Доступ к общедоступной информации является открытым и ее использование не может нанести вреда ИС.

Информация ограниченного доступа должна подвергаться защите от воздействия различных событий, явлений, как внутренних так и внешних,

способных в той или иной мере нанести ущерб данной информации.

Доступ к подобной информации имеют работники тех структурных подразделений, которые отвечают за сбор и обработку служебной информации.

С них берется подписка о ее не разглашении, начальником отдела кадров.

Ответственность за разглашение информации устанавливается Федеральным законом N149-ФЗ от 27.07.2006г «Об информации, информационных технологиях. О защите информации.(с изменениями на 21 июля 2014 года)

И положением колледжа « Об обработке и защите персональных данных работников» утвержденных 01.09.2014 г.

К любому сотруднику колледжа, нарушившему подписку, могут быть применены дисциплинарные меры.

2.Мероприятия по обеспечению безопасности информации

2.1 Ограничения физического доступа к средствам вычислительной техники

- Устанавливать решетки, сигнализацию, не допускающие кражу оборудования.
- Выдавать ключи от кабинетов, только ответственным лицам, закрыть не санкционированный доступ в учебные классы
- Устанавливать пожарную систему, не допускающую физическое разрушение оборудования
- Правильно устанавливать оборудование (компьютерные столы, удаленность от батарей, влажность)
- Проводить своевременно ремонтные и восстановительные работы компьютерного оборудования

2.2 Ограничения к информационным ресурсам

•Устанавливать лицензионные операционные системы и прикладное программное обеспечение

• Разрешить обновление лицензионных систем с сайта производителя. Следить за выпуском обновлений прикладного программного обеспечения

• После установки операционной системы и необходимого софта, задействовать функцию сохранения и восстановления информации. Так можно быстро восстановить операционную систему при сбоях.

• Вход в систему с учетной записью АДМИНИСТРАТОР делать с паролем, менять пароль в начале каждого семестра обучения

• Разрешить вход в систему студентам только под учетной записью Гость, что б студенты не смогли изменить системные файлы, удалить их.

• Возвращать базовые настройки операционных систем и прикладных программ.(Они могут быть изменены в ходе обучения)

• Устанавливать на каждом рабочем месте Антивирус- Касперского и регулярно обновлять ключ защиты(ежемесячный, по подписке) и антивирусные базы. Сканировать жесткие диски после каждого обновления баз

• Не публиковать в интернете подробную информацию о себе.

• Менять пароли к электронному почтовому ящику 1 раз в 6 месяцев

• Подключать компьютеры к сети через стабилизатор напряжения, а лучше — через источник бесперебойного питания. Этим снижается вероятность того, что после очередного скачка напряжения важная информация будет уничтожена.

• Архивировать данные. Хранить резервные копии самых важных документов и баз данных на внешнем носителе.

•Регулярно обновлять пакеты прикладных программ АСУ (1С. БашФин, Референт, Налогоплательщик)

•Следить за сроком действия Электонно -цифровых подписей

Не передавать файлы содержащие отчеты, списки сотрудников и сведения о них, таблицы расчетов заработной платы посторонним лицам. Распечатки этих файлов не выбрасывать без уничтожения и не пользоваться ими как черновиками. Делать в системе заставку экрана 1 мин., для того чтобы не сканировалась информация с экрана. Задавать для директорий с важными документами разграничения доступа.

Так защищаются документы от нежелательного просмотра, а также предотвратите их случайное удаление или изменение. Проверять на наличие вирусов всю поступающую информацию, особенно с внешних накопителей. Конфиденциальная информация колледжа или сторонних организаций или не хранить и не передавать на компьютеры, не принадлежащие колледжу. Политика информационной безопасности пересматривается один раз в 3 года либо в случаях изменения технического и программного обеспечения колледжа.

РАЗРАБОТАНО:

Инженер программист 1 кат. 01.09.14 (Рындина В.П.)
(дата) (полнись)

СОГЛАСОВАНО:
Зам.директора 01.09.14 /(Шайхетдинова Л.М.)
(дата) (подпись)

Юрисконсульт 01.09.14г /(Медведева Е.М.)
(дата) (полнись)