ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «СЕТЕВОЙ ЭТИКЕТ И БЕЗОПАСНОСТЬ СЕТИ»

Направленность: техническая
Возраст обучающихся: 16-18 лет
Количество часов на освоение: 72 час.

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Нормативно-правовая база:

Федеральный закон от 29.12.2012г. № 273 «Об образовании в Российской Федерации»;

Указ Президента Российской Федерации от 7 мая 2012г. № 599 «О мерах по реализации государственной политики в области образования и науки»;

Указ Президента Российской Федерации от 7 июля 2011г. № 899 Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации;

Приказ Министерства образования и науки Российской Федерации от 29 августа 2013г. № 1008 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

Приказ Министерства образования и науки Российской Федерации от 28 июля 2014г. № 805 «Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.01 «Организация и технология защиты информации»;

Приказ Министерства образования и науки Российской Федерации от 13.08.2014г. № 1000 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.02 Информационная безопасность телекоммуникационных систем»;

Разъяснения к приказу Минобрнауки от 29 августа 2013 г. N 1008 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

Письмо Минобрнауки России № 09-3242 от 18.11.2015 «О направлении информации» (вместе с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)».

1.2. Область применения программы

Программа профессиональной подготовки «Сетевой этикет и безопасность сети» направлена на освоение и развитие профессиональных компетенций по направлениям:

1. Использование правил общения в сети Интернет;

2. Участие в планировании и организации работ по обеспечению защиты объекта;

3. Организация и технология работы с конфиденциальными документами;

4. Применение программно-аппаратных и технических средств защиты информации;

5. Участие в организации комплексной системы защиты объекта.

Рабочая программа может быть использована в дополнительном профессиональном образовании в рамках реализации программ переподготовки и дополнительной подготовки кадров в учреждениях СПО.

1.3. Цели и задачи программы:

В результате овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся должен:

Уметь:

- Применять основы правовых знаний в различных сферах жизнедеятельности:

- применять нормативные документы в сфере информационной безопасности и защиты информации при определении категории доступа к информации организации, а также для ее защиты;
- выявлять уязвимости активов организации;
- оценивать состояние организационной защиты информации;

- Использовать нормативно-правовые документы, международные и отечественные стандарты в области безопасности информационных систем и технологий:

- определять виды активов организации;
- определять ценность каждого актива организации;
- формулировать требования к обеспечению сотрудниками защиты информации.

- Проводить обследования организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе:

- определять группы и содержание угроз активам организации;
- формировать экспертное заключение о соотношении уровня угроз, уязвимостей и ценности активов.

- Выполнять технико-экономическое обоснование проектных решений:

- определять комплекс средств обеспечения информационной безопасности и защиты информации;
- рассчитывать величину потерь вследствие реализации угроз информационной безопасности;
- рассчитывать объем разового и постоянного ресурса, выделяемого на защиту информации;
- определять затраты на модернизацию системы информационной безопасности и срок окупаемости вложенных средств.

Знать:

- Основы использования правовых знаний в различных сферах жизнедеятельности:

- основные правовые понятия, правовые акты Российской Федерации в области защиты информации;

- правовые нормы и стандарты по лицензированию в области обеспечения защиты коммерческой и государственной тайны и сертификации средств защиты информации;

- руководящие документы по оценке защищенности компьютерных систем;

- основные руководящие документы по обеспечению режима и секретности (конфиденциальности) в организации.

- Порядок использования нормативно-правовых документов, международных и отечественных стандартов в области информационных систем и технологий:

- основные термины и понятия информационной безопасности;

- направления обеспечения информационной безопасности;

- действия, приводящие к незаконному овладению информацией;

- виды тайн как объекта защиты;

- компоненты и уровни системы информационной безопасности;

- порядок защиты информационных активов;

- основные положения политики информационной безопасности.

- Методы проведения обследования организаций, выявления информационных потребностей пользователей, формирования требования к информационной системе

- основы организационной защиты информации, ее современные проблемы и терминологию;

- основные организационные и административные меры обеспечения защиты информации;

- типовую структуру службы безопасности, ее основные задачи и функции должностных лиц.

- Требования к выполнению технико-экономического обоснования проектных решений:

- основные требования к системе защиты информации;

- классификацию средств обеспечения информационной безопасности и защиты информации;
- соотношение угроз и адекватных средств обеспечения информационной безопасности и защиты информации;
- физические каналы утечки информации и соответствующие способы защиты;
- методы анализа эффективности систем информационной безопасности и защиты информации.

1.4. Количество часов на освоение программы подготовки:

Всего – 72 часа, в том числе:

- максимальная учебная нагрузка обучающегося — 72 часа,

в том числе:

- обязательную аудиторную учебную нагрузку обучающегося — 72 часа.

1.5. Режим занятий

Режим занятий обучающихся регламентируется календарным учебным графиком и расписанием занятий.

Единицей измерения учебного времени и основной формой организации учебной работы является учебное занятие. Учебные занятия ведутся на базе колледжа. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут. Занятия проводятся в форме пары - двух объединенных академических часов с перерывом продолжительностью 10 мин.

Продолжительность занятия с использованием компьютерной техники организуются в соответствии с гигиеническими требованиями к ПЭВМ и организации работы.

Изменение режима работы занятий определяется приказом директора в соответствии с нормативно-правовыми документами.

1.6. Срок реализации программы

Программа рассчитана на 1 год обучения в количестве 72 аудиторных часов. В программе выделены два этапа обучения в форме разделов.

Запланированный срок реализации программы реален для достижения результатов.

1.7. Категории обучающихся

Учебная группа формируется из граждан, изъявивших желание на обучение по данной программе. Возраст обучающихся составляет 16-18 лет.

Программа предназначена для лиц, обладающих уровнем базового образования по информатике, математике и физике.

Наполняемость группы определяется количеством рабочих мест в лаборатории для получения навыков по использованию полученных теоретических знаний в количестве 15 человек

1.8. Форма занятий

Форма организации занятий групповая. При изучении тем, содержащих практические занятия – индивидуальная.

1.9. Отличительная особенность программы

В данной программе материалы подобраны с целью легкого и понятного усвоения их обучающимися с разным уровнем подготовки по построению компьютерных сетей, используемого сетевого оборудования, программного обеспечения.

В 1 разделе программы изучаются основные понятия сетевого этикета основы психологии в сети, ведение общения через социальные сети.

Во 2 разделе разбираются принципы организации работ по обеспечению информационной безопасности систем.

1.10. Формы контроля.

Отслеживание результативности занятий, включающее: ведение конспектов, выполнение практических работ, контрольных заданий и тестов;

Система оценочных средств позволяет проконтролировать результат обучения, измерить его и оценить.

Виды контроля:

-начальный (или входной контроль) проводится с целью определения уровня развития обучающихся;

-текущий контроль – с целью определения степени усвоения обучающимися учебного материала;

-промежуточный контроль – с целью определения результатов обучения;

-итоговый контроль – с целью определения изменения уровня развития обучающихся.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

Результатом освоения программы является овладение обучающимися ВПД «**Сетевой этикет и безопасность сети»**, в том числе профессиональными компетенциями:

Код	Наименование результата обучения
ПК 1.1.	Участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.
ПК 1.2.	Участвовать в разработке программ и методик организации защиты информации на объекте.
ПК 1.3.	Осуществлять планирование и организацию выполнения мероприятий по защите информации.
ПК 1.4.	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.
ПК 1.5.	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.
ПК 1.6.	Обеспечивать технику безопасности при проведении организационно-технических мероприятий.
ПК 1.7.	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.
ПК 1.8.	Проводить контроль соблюдения персоналом требований режима защиты информации.
ПК 1.9.	Участвовать в оценке качества защиты объекта.
ПК 2.1.	Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.
ПК 2.2.	Организовывать и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.
ПК 2.3.	Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.
ПК 2.4.	Организовывать архивное хранение конфиденциальных документов.
ПК 2.5.	Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.
ПК 2.6.	Вести учет работ и контроль объектов, подлежащих защите.
ПК 2.7.	Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.
ПК 2.8.	Документировать ход и результаты служебного расследования.
ПК 2.9.	Использовать нормативные правовые акты, нормативно-

	методические документы и справочную документацию по защите информации.
ПК 3.1.	Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
ПК 3.2.	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
ПК 3.3.	Фиксировать отказы в работе средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ПК 4.1.	Участвовать в разработке организационной структуры комплексной системы защиты информации.

3. Содержание обучения по программе «СЕТЕВОЙ ЭТИКЕТ И БЕЗОПАСНОСТЬ СЕТИ»

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Сетевой этикет		**24**	
Тема 1.1. Виды и основы сетевого этикета.	**Содержание учебного материала**	**8**	
	1.1.1.Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Правила общения в Интернете.	2	2
	1.1.2.Основы сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.	2	2
	1.1.3.Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми	2	2
	1.1.4.**Практическое занятие № 1.** Создание виртуальной личности и ведение общения в Интернете с соблюдением этикета.	2	2
Тема 1.2. Психологическая обстановка в Интернете.	**Содержание учебного материала**	**6**	
	1.2.1.Основы психологии в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид	2	2
	1.2.2.Общение в сети и его последствия. Агрессия в сети. Психологическое влияние через Интернет.	2	2
	1.2.3.**Практическое занятие № 2.** Методы защиты от агрессии и психологического влияния через Интернет.	2	2
Тема 1.3. Общение в социальных сетях.	**Содержание учебного материала**	**6**	
	1.3.1.Анонимность в сети. Общение в социальных сетях. Правила поведения в скайпе	2	2
	1.3.2.Форум и переписка в сети. Этикет при переписке. Модерация.	2	2
	1.3.3.**Практическое занятие № 3.** Переписка с участием модератора.	2	2
Тема 1.4. Этикет и безопасность	**Содержание учебного материала**	**4**	
	1.4.1.Безопасная работа в сети в процессе сетевой коммуникации (чаты,	2	2

сети.	форумы, социальные сети, конференции, скайп и пр.).		
	1.4.2.Безопасная работа при работе в локальных и глобальной компьютерных сетях.	2	2
Раздел 2. Информационная безопасность компьютерных сетей		**48**	
Тема 2.1.Организационное и правовое обеспечение информационной безопасности	**Содержание учебного материала**	**4**	
	2.1.1.Законодательный уровень информационной безопасности. Основные понятия, термины и определения в области защиты информации.	2	2
	2.1.2.Международные и российские стандарты безопасности информационных систем. Стандарт, базирующиеся на процессном подходе к обеспечению информационной безопасности – ISO.	2	2
Тема 2.2. Угрозы информационной безопасности.	**Содержание учебного материала**	**4**	
	2.2.1.Наиболее распространенные угрозы. Основные определения и критерии классификации угроз.	2	2
	2.2.2.Основные направления защиты информации.	2	2
Тема 2.3. Политика и аудит информационной безопасности	**Содержание учебного материала**	**4**	
	2.3.1.Политика безопасности. Организация ИБ. Цели и задачи Политики информационной безопасности. Общая структура Политики информационной безопасности.	2	2
	2.3.2.Аудит состояния информационной безопасности на предприятии. Порядок проведения аудита информационной безопасности в компании.	2	2
Тема 2.4. Управление рисками информационной безопасности. Подразделение информационной безопасности.	**Содержание учебного материала**	**12**	
	2.4.1.Управление рисками информационной безопасности.	2	2
	2.4.2.Подготовительные этапы управления рисками. Основные этапы управления рисками.	2	2
	2.4.3.Организация реагирования на чрезвычайные ситуации (инциденты).	2	2
	Программная поддержка анализа рисков.	2	2
	2.4.4.**Практическое занятие № 4.** Анализ программ управления рисками в информационных сетях.	2	2
	2.4.5.Подразделение информационной безопасности.	2	2
Тема 2.5. Защита информации при работе в сети Internet.	**Содержание учебного материала**	**12**	
	2.5.1.Возможность защиты информации при работе в сети Internet. Межсетевое экранирование.	2	2

	2.5.2.VPN (виртуальная частная сеть). Преимущества организации виртуальных частных сетей на основе Internet.	2	2
	2.5.3.**Практическое занятие № 5.** Установка VPN и работа в виртуальной частной сети.	2	2
	2.5.4.«Облачные» технологии.	2	2
	2.5.5.Программные средства, поддерживающие управление информационной безопасностью на предприятии.	2	2
	2.5.6.Использование программных средств для поддержки управления безопасностью. Программная поддержка работы с политикой безопасности.	2	2
Тема 2.6. Методы и средства защиты компьютерных систем.	**Содержание учебного материала**	**6**	
	2.6.1.Основы криптографической защиты информации. Классификация методов криптографического закрытия информации.	2	2
	2.6.2.**Практическое занятие № 6.** Использование криптографической защиты информации при передаче информации по сети.	2	2
	2.6.3.Электронная подпись. Электронная подпись как базовый механизм обеспечения юридической силы документа при электронном документообороте.	2	2
Тема 2.7. Противодействие промышленному шпионажу. Техническая защита информации. Режим коммерческой тайны.	**Содержание учебного материала**	**4**	
	2.7.1. Классификация технических каналов утечки информации: утечка и защита акустической (речевой) информации; побочные электромагнитные излучения и наводки (ПЭМИН) и методы защиты информации от утечки через ПЭМИН.	2	2
	2.7.2. Средства и методы обнаружения технических каналов утечки информации. Мероприятия по выявлению технических каналов утечки информации (ТКУИ). Оценка защищенности информации от утечки по ТКУИ.	2	2
	Дифференцированный зачет.	**2**	
	Всего:	**72**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Минимальное материально-техническое обеспечение

Для реализации программы имеется учебный кабинет**,** оснащенный компьютерами с соответствующим программным обеспечением.

4.2. Информационное обеспечение обучения.

Перечень учебных изданий, дополнительной литературы, Интернет – ресурсов

Основные источники:

№ п/п	Наименование	Автор	Издательство и год издания
1	Общение в сети Интернет. Просто как дважды два.	Аксак В.А.	М.: Эксмо, 2006
2	Энциклопедия студента.	Кузнецов И.Н.	Минск: Книжный дом. 2004.
3	Современный этикет и деловой протокол: учебное пособие.	Соловьев Э.Я. -	М.: Интелл Синтез, 2004.
	Организационно-правовое обеспечение информационной безопасности. Учебное пособие.	Под ред. Стрельцова А.А.	М.: Издательский центр «Академия», 2008.
6	Компьютерные сети. Принципы, технологии, протоколы: учеб. Для вузов. – 4-е изд.	Олифер В.	СПб: Питер, 2010.

Интернет – ресурсы

1. Компьютерные сети // Информатика и информационно – коммуникационные технологии [Электронный ресурс]. – Режим доступа: http://www.kolomna school7-ict.narod.ru/index.htm
2. Основные компоненты и разновидности компьютерных сетей / Полноценные статьи и короткие заметки системного администратора Windows, сетях, железе и компьютерной безопасности [Электронный ресурс]. – Режим доступа: http://blogsisadmina.ru/seti/osnovnye-komponenty-i-raznovidnosti kompyuternyx-setej.html
3. Сетевой этикет // Энциклопедия знаний: электронное справочное пособие [Электронный ресурс]. – Режим доступа: http://www.pandia.ru/text/77/211/89142.php
4. Этика сетевого общения // Федеральная стажировочная площадка. Достижение нового качества образования через развитие информационной инфраструктуры Алтайского края [Электронный ресурс]. – Режим доступа: http://fsp.akipkro.ru/20

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
В результате освоения программы обучающийся должен уметь:		Проведение текущего контроля, дифференцированного зачета Оценка результатов деятельности обучающихся на занятиях. Методы оценки результатов обучения: - традиционная система оценок в баллах, выставление итоговой оценки на основе промежуточной аттестации; - мониторинг промежуточного контроля.
пользоваться аппаратурой систем контроля доступа;	ПК 1.2	
выделять зоны доступа по типу и степени конфиденциальности работ; защиты информации;	ПК 1.3	
определять порядок организации и проведения рабочих совещаний;	ПК.1.4	
использовать критерии подбора и расстановки сотрудников подразделений защиты информации;	ПК.1.6	
организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;	ПК.1.7	
проводить инструктаж персонала по организации работы с конфиденциальной информацией;	ПК.1.8	
контролировать соблюдение персоналом требований режима	ПК.1.9	
использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	ПК.2.1	
разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;	ПК.2.2	
документировать ход и результаты служебного расследования;	ПК.2.3	
определять состав документируемой конфиденциальной информации;	ПК.2.4	
подготавливать, издавать и учитывать конфиденциальные документы;	ПК.2.5	
составлять номенклатуру конфиденциальных дел;	ПК.2.6.	
формировать и оформлять конфиденциальные дела;	ПК.2.7	

организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;	ПК.2.8	
использовать системы электронного документооборота;	ПК.2.9	
Вести безопасносное общение в общественных сетях	ПК.1.1.	
В результате освоения программы обучающийся должен знать:		
правовые основы защиты конфиденциальной информации по видам тайны;	ОК 1-12	
порядок лицензирования деятельности по технической защите конфиденциальной информации;	ОК 1-12	
правовые основы деятельности подразделений защиты информации;	ОК 1-12	
правовую основу допуска и доступа персонала к защищаемым сведениям;	ОК 1-12	
правовое регулирование взаимоотношений администрации и персонала в области защиты информации;	ОК 1-12	
систему правовой ответственности за утечку информации и утрату носителей информации;	ОК 1-12	
правовые нормы в области защиты интеллектуальной собственности;	ОК 1-12	
порядок отнесения информации к разряду конфиденциальной информации;	ОК 1-12	
порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;	ОК 1-12	
организацию конфиденциального документооборота;	ОК 1-12	
технологию работы с конфиденциальными документами;	ОК 1-12	
организацию электронного документооборота	ОК 1-12	