Государственное профессиональное образовательное учреждение
Ярославской области
Ярославский градостроительный колледж

УТВЕРЖДАЮ:
Директор колледжа
_____ Зуева М.Л.
«__» _____ 2019г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«Основы информационной безопасности»

Возраст обучающихся: 15-18 лет
Срок реализации: 4 месяца

Введено в действие с — 01.09.2019

Номер экземпляра: 1

Место хранения: ЦДПП

Ярославль, 2019 г.

Лист согласования

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
«Основы информационной безопасности»

СОГЛАСОВАНО:

кафедра ИТ **Руководитель кафедры:**

«26» 08 2019 г. Протокол № 1 _____ **Неделяева Н. А.**
подпись Фамилия И.О.

Автор-разработчик:

Тимощук М.В. – преподаватель высшей категории

Реестр рассылки

№ учтенного экземпляра	Подразделение	Количество копий
1.	Кафедра ИТ	1
2.		1

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Нормативно-правовые основы разработки программы.

Настоящая дополнительная общеобразовательная общеразвивающая программа «Основы информационной безопасности» (далее - программа) разработана с учетом:

– Федерального закона от 29.12.12 г. No273-ФЗ «Об образовании в Российской Федерации»;

– приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 09 ноября 2018 г. No 196 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

– Концепции развития дополнительного образования детей в Российской Федерации, утвержденной распоряжением Правительства РФ от 4.09.2014 г. No 1726-р;

– санитарно-эпидемиологическими правил и нормативов 2.4.4.3172-14 «Требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей (утв. Главным государственным санитарным врачом РФ от 04.07.2014 г. No 41);

– Письма Минобрнауки РФ от 11.12.2006г. №06-1844 «О примерных требованиях к программам дополнительного образования детей»;

– Письма Минобрнауки РФ от 18.11.2015г. №09-3242 «Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»

– Государственной программы РФ «Развитие образования на 2013-2020 годы, утвержденной постановлением Правительства РФ от 15.04.2014 г. No 295;

– Устава государственного профессионального образовательного учреждения Ярославской области Ярославского градостроительного колледжа.

1.2. Направленность программы

Дополнительная общеобразовательная общеразвивающая программа «Основы информационной безопасности» относится к программам технической направленности.

1.3. Цели и задачи образовательной программы

Цель – Формирование профессиональных компетенций, необходимых в практической работе по защите информации

Задачи

Обучения:

- Освоение понятия информационная безопасность
- Освоение принципов и методов обеспечения информационной безопасности
- Формирование навыков расшифровки текста различными методами шифрования
- Формирование навыков шифрования, используя специальное программное обеспечение

Развития:

- Повышение интереса к будущей профессии
- Приобретение навыков самостоятельной работы
- Развитие способности к исследовательской деятельности

Воспитания:

- Воспитание культуры в области применения ИКТ в различных сферах человеческой деятельности
- Воспитание нравственных качеств, негативного отношения к нарушителям информационной безопасности.

1.4. Актуальность, новизна и значимость программы.

Актуальность программы обусловлена тем, что в период глобального процесса информатизации общества возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств информационно-коммуникационных технологий. Мировое сообщество стоит перед глобальной проблемой – проблемой обеспечения информационной безопасности. Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователей, компетентных в сфере защиты информации.

Дополнительная общеразвивающая программа «Основы информационной безопасности» направлена на развитие компетенций:

1 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

3. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

4. Осуществлять профилактические мероприятия по защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.

5. Разрабатывать меры по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программнотехнические комплексы;

6. Выполнять работы по созданию, редактированию, оформлению, сохранению, передаче информационных объектов различного типа с помощью современных программных средств

1.5 Отличительные особенности образовательной программы.

Реализуется на базе среднего профессионального образовательного учреждения. Образование ориентировано на подготовку учащихся к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопросы обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны.

1.6 Категория обучающихся:

Программа предназначена для учащихся от 15 до 18 лет. Обучаться по данной программе может любой желающий, при отсутствии медицинских противопоказаний. Специальных знаний и предварительной подготовки для зачисления в группу не требуется.

Прием производится на основания договора об образовании на обучение по дополнительным образовательным услугам.

1.7 Условия и сроки реализации образовательной программы.

К занятиям допускаются студенты без специального отбора.

Наполняемость группы не менее 10 и не более 25 человек.

Режим занятий: 1 раза в неделю по 2 академических часа (по 45 минут) с 10 минутным перерывом.

Объем учебной нагрузки в год – 40 часов, в неделю – 2 часа.

Занятия проводятся в кабинете Информационной безопасности.

Форма обучения – очная.

Форма занятий - групповая, по подгруппам. Виды занятий указаны в разделе 4.

Форма аттестации – промежуточная, с применением различных видов контроля.

1.8. Календарный учебный график

№ п/п	Месяц	Форма занятия	Кол-во часов	Тема занятия	Место проведения
1.	Сентябрь 1 день	По подгруппам	2	Актуальность проблемы обеспечения безопасности ИТ	ул. Чайковского, д.55
2.	Сентябрь 2 день	По подгруппам	2	Понятие угрозы информационной безопасности. Каналы утечки информации.	ул. Чайковского, д.55
3.	Сентябрь 3 день	По подгруппам	2	Общие сведения о вредоносных программах. Компьютерные вирусы. Профилактика заражения.	ул. Чайковского, д.55
4.	Сентябрь 4 день	По подгруппам	2	Методы защиты компьютеров от вредоносных программ. Антивирусные программы.	ул. Чайковского, д.55
5.	Сентябрь 5 день	По подгруппам	2	Восстановление информации.	ул. Чайковского, д.55
6.	Октябрь 6 день	По подгруппам	2	Законодательство в области защиты информации.	ул. Чайковского, д.55
7.	Октябрь 8 день	По подгруппам	2	Защита информации ограниченного доступа.	ул. Чайковского, д.55
8.	Октябрь 7 день	По подгруппам	2	Основные сервисы безопасности	ул. Чайковского, д.55
9.	Октябрь 9 день	По подгруппам	2	Правила создания и замены паролей. Идентификация и аутентификация.	ул. Чайковского, д.55
10.	Октябрь 10 день	По подгруппам	2	Технические средства защиты информации.	ул. Чайковского, д.55
11.	Ноябрь 11 день	По подгруппам	2	Безопасность в сети Интернет. Защита электронного обмена данных в Интернете.	ул. Чайковского, д.55
12.	Ноябрь 12 день	По подгруппам	2	Способы отделения интрасети от глобальных сетей.	ул. Чайковского, д.55
13.	Ноябрь 13 день	По подгруппам	2	Фильтрующий маршрутизатор, программный фильтр, системы типа FireWal.	ул. Чайковского, д.55
14.	Ноябрь 14 день	По подгруппам	2	Информационно–психологическая безопасность личности в информационном обществе.	ул. Чайковского, д.55
15.	Ноябрь 15 день	По подгруппам	2	Виртуальная реальность и её воздействие на здоровье человека.	ул. Чайковского, д.55
16.	Декабрь 16 день	По подгруппам	2	Элементы шифрования	ул. Чайковского, д.55
17.	Декабрь 17 день	По подгруппам	2	Элементы криптоанализа	ул. Чайковского, д.55

18.	Декабрь 18 день	По подгруппам	2	Шифрование методам подстановки	ул. Чайковского, д.55
19.	Декабрь 19 день	По подгруппам	2	Шифровальная система Вижинера	ул. Чайковского, д.55
20.	Декабрь 20 день	По подгруппам	2	Перспективные направления в области обеспечения информационной безопасности	ул. Чайковского, д.55

1.9. Планируемые результаты и способы определения результативности образовательного процесса.

Планируемые результаты

Обучающийся будет знать:

- - основные понятия и определения из области обеспечения информационной безопасности;
- методы и средства борьбы с угрозами информационной безопасности;
- классификацию вредоносных программ и их влияние на целостность информации; порядок заражения файлов;
- методы проведения профилактики, защиты и восстановления пораженных вредоносными программами объектов;
- нормативные руководящие документы, касающиеся защиты информации, существующие стандарты информационной безопасности;
- принципы выбора пароля, аппаратные и программные средства для аутентификации по паролю;
- основные понятия криптографических методов защиты информации, механизмы цифровой электронной подписи;
- существующие программные продукты, предназначенные для защиты электронного обмена данными в Интернете, способы отделения интрасети от глобальных сетей;
- нормы информационной этики и права.

уметь:

- - объяснять необходимость изучения проблемы информационной безопасности;
- применять методы профилактики и защиты информационных ресурсов от вредоносного программного обеспечения;
- восстанавливать повреждённую информацию;
- соблюдать права интеллектуальной собственности на информацию;
- применять методы ограничения, контроля, разграничения доступа, идентификации и аутентификации;
- использовать современные методы программирования для разработки сервисов безопасности;
- производить простейшие криптографические преобразования информации;
- применять простейшие методы шифрования информации;

- планировать организационные мероприятия, проводимые при защите информации;
- применять методы защиты информации в компьютерных сетях;
- различать основные виды информационно-психологических воздействий в виртуальной реальности;
- соблюдать требования информационной безопасности, этики и права;
- искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества;
- интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои суждения по проблемным вопросам;
- сравнивать, анализировать и систематизировать имеющийся учебный материал;
- участвовать в групповой работе и дискуссиях, решении задач в игровых ситуациях и проектной деятельности;
- представлять результаты учебных исследовательских проектов с использованием информационно-коммуникационных технологий.

Способы отслеживания результатов освоения программы учащимися:
- проверка выполнения задания по образцу;
- промежуточный контроль усвоения разделов программы с помощью выполнения зачетных заданий;
- промежуточный контроль усвоения материала путем тестирования.

Результаты обучения оцениваются по пятибалльной системе

Учебно-тематический план

№	Раздел и темы	Количество часов				Форма контроля
		Теория	Практика	Самостоятельная подготовка	Всего	
	Тема 1. Основные понятия информационной безопасности	**0**	**20**	**10**	**30**	
1	Актуальность проблемы обеспечения безопасности ИТ		**2**	**1**	**3**	оценка выполнения практического задания
2	Понятие угрозы информационной безопасности. Каналы утечки информации.		2	1	3	оценка выполнения практического задания
3	Общие сведения о вредоносных программах. Компьютерные вирусы. Профилактика заражения.		2	1	3	оценка выполнения практического задания
4	Методы защиты компьютеров от вредоносных программ. Антивирусные программы.		2	1	3	оценка выполнения практического задания
5	Восстановление информации.		2	1	3	оценка выполнения практического

						задания
6	Законодательство в области защиты информации.		2	1	3	оценка выполнения практического задания
7	Защита информации ограниченного доступа.		2	1	3	оценка выполнения практического задания
8	Основные сервисы безопасности		2	1	3	оценка выполнения практического задания
9	Правила создания и замены паролей. Идентификация и аутентификация.		2	1	3	оценка выполнения практического задания
10	Технические средства защиты информации.		2	1	3	оценка выполнения практического задания
	Тема 2. Защита информации в компьютерных сетях.	**0**	**10**	**5**	**15**	
11	Безопасность в сети Интернет. Защита электронного обмена данных в Интернете.		2	1	3	оценка выполнения практического задания
12	Способы отделения интрасети от глобальных сетей.		2	1	3	оценка выполнения практического задания
13	Фильтрующий маршрутизатор, программный фильтр, системы типа FireWal.		2	1	3	оценка выполнения практического задания
14	Информационно–психологическая безопасность личности в информационном обществе.		2	1	3	оценка выполнения практического задания
15	Виртуальная реальность и её воздействие на здоровье человека.		2	1	3	оценка выполнения практического задания
	Тема 3. Криптографическое преобразование информации.	**0**	**10**	**5**	**15**	
16	Элементы шифрования		2	1	3	оценка выполнения практического задания
17	Элементы криптоанализа		2	1	3	оценка выполнения практического задания
18	Шифрование методам подстановки		2	1	3	оценка выполнения практического задания
19	Шифровальная система Вижинера		2	1	3	оценка выполнения

						практического задания
20	Перспективные направления в области обеспечения информационной безопасности		2	1	3	оценка выполнения зачетного задания
	Итого		**40**	**20**	**60**	

1. Содержание образовательной программы

Тема 1. Основные понятия информационной безопасности (20 часов)

Практика: Общие проблемы информационной безопасности. Классификация угроз информационной безопасности. Вредоносные программы. Методы профилактики и защиты. Правовые основы обеспечения информационной безопасности. Современные методы защиты информации в автоматизированных системах обработки данных. Технические и организационные методы защиты информации

Самостоятельная подготовка: Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Отечественные и зарубежные стандарты в области информационной безопасности. Электронная цифровая подпись. Контроль целостности; экранирование; анализ защищённости; обеспечение отказоустойчивости; обеспечение безопасного восстановления.

Тема 2. **Защита информации в компьютерных сетях** ***(10 часов)***

Практика: Примеры взломов сетей и веб-сайтов. Причины уязвимости сети Интернет. Цели, функции и задачи защиты информации в компьютерных сетях. Безопасность в сети Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д. Определение понятия информационно-психологической безопасности. Основные виды информационно-психологических воздействий. Виртуальная реальность и её воздействие на нравственное, духовное, эмоциональное и физическое здоровье человека.

Самостоятельная подготовка:Методы атак, используемые злоумышлиниками для получения или уничтожения интересующей информации через Интернет. Игромания, компьютерные манипуляции, фишинг, киберугрозы и пропаганда других опасных явлений в Интернете. Способы Защиты от нежелательной информации в Интернете. Нравственно-этические проблемы информационного общества.

Тема 3. **Криптографическое преобразование информации** ***(10 часов)***

Практика: Понятие криптографического преобразования информации. Простейшие шифры и их свойства. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Элементы шифрования. Шифрование методам подстановки. Шифровальная система Вижинера. Перспективные направления в области обеспечения информационной безопасности.

Самостоятельная подготовка: История криптографии. Шифрование методом замены, скрытия, аффинным шифрованием. Шифровальная система Хилла. Использование специальных инструментов шифрования: Audacuty, StegSolve, Sonic Visualiser.

4.Организационно-педагогические условия

4.1. Методическое обеспечение программы.

При организации обучения используется личностно-ориентированный, компетентностный и дифференцированный подход. На занятиях используются следующие педагогические технологии: исследовательский метод, проблемное обучение и разноуровневое обучение. Образовательная программа содержит практическую и самостоятельную подготовку, большее количество времени уделяется выработке практических навыков.

Формы занятий: интегрированные, тестирование, индивидуальная работа с использованием компьютерной и мультимедийной техники.

Кроме традиционных методов используются элементы индивидуального проекта и игровых технологий.

Оценка образовательных результатов по итогам освоения программы проводится в форме итоговой аттестации. Основная форма аттестации – итоговая оценка.

Оценка образовательных результатов проводится в форме выполнения зачетных заданий по темам.

Мониторинг образовательных результатов

Система отслеживания, контроля и оценки результатов обучения по данной предусматривает определение начального уровня знаний, умений и навыков обучающихся, текущий контроль в течение занятий, итоговый контроль. Входной контроль осуществляется на первых занятиях с помощью наблюдения педагога за работой обучающихся. Текущий контроль проводится с помощью различных форм... Цель текущего контроля – определить степень и скорость усвоения каждым обучающимся материала и скорректировать программу обучения, если это требуется. Итоговый контроль проводится в конце обучения. Итоговый контроль определяет фактическое состояние уровня знаний, умений, навыков обучающегося, степень освоения материала по каждому изученному разделу и всей программе. Формы подведения итогов обучения: выполнение зачетных заданий и тестирование по темам.

Среди инструментов оценки образовательных результатов применяются:

- контрольно-измерительные материалы (Приложение 1);

4.2. Материально-техническое обеспечение программы.

В состав перечня оборудования входит программное обеспечение:
- Операционная система Windows;
- Пакет программ Microsoft Office;
- Антивирусная программа Касперский;

технические средства обучения:
- Персональные компьютеры, объединенные в локальную сеть с высокоскоростным доступом в Internet
- Экран и мультимедийный проектор или ЖК-панель;

4.3. Кадровое обеспечение программы

Программу реализуют преподаватели специализированных дисциплин кафедры Информационных технологий.

6. Список литературы и иных источников

Основная литература для педагога:

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 2017.
2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2016.
3. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2017. – 212 с.

Дополнительная литература для педагога:

4. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь» 2016.
5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. –МЦНМО, 2017.

Основная литература для обучающихся:

1. Алферов А.П. Основы криптографии. Учебное пособие. - М.: Гелиос АРВ, 2017
2. Кукина Е.Г., Романьков В.А. Сборник задач и упражнений по криптографии. –М.: Форум, 2016

3. Интернет-ресурсы для обучающихся:

1. Основы информационной безопасности и защиты информации - [Электронный ресурс] // mail@texterra.ru. Режим доступа: https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1, свободный
2. Основы информационной безопасности и защиты информации - [Электронный ресурс] // securitylab.ru. Режим доступа: https://www.securitylab.ru /, свободный
3. Основы информационной безопасности и защиты информации - [Электронный ресурс] // ПИРИТ. Режим доступа: https:// https://pirit.biz/reshenija/informacionnaja-bezopasnost, свободный

Приложение 1

Контрольно-измерительные материалы

Примеры заданий:

Задание 1

1. Маша и Яша играют в “шифровку”. Маша придумывает правило преобразования текста. Яша может говорить Маше любые слова иузнавать, как они звучат в зашифрованном виде. Задача Яши – отгадать задуманное правило шифрования. Перед вами слова, которые говорил Яша и их шифр. РЫБА - ОЩЯЮ ЕНОТ - ГЛМР А – Ю ДИКОБРАЗ - ВЖИМЯОЮЁ Угадайте, как зашифровать слово ЯБЛОКО. Ответ запишите заглавными буквами.

2. Вася шифрует русские слова, записывая вместо каждой буквы её номер в алфавите (без пробелов). Номера букв даны в таблице:

А 1	Й 11	У 21	Э 31
Б 2	К 12	Ф 22	Ю 32
В 3	Л 13	Х 23	Я 33
Г 4	М 14	Ц 24	
Д 5	Н 15	Ч 25	
Е 6	О 16	Ш 26	
Ё 7	П 17	Щ 27	
Ж 8	Р 18	Ъ 28	
З 9	С 19	Ы 29	
И 10	Т 20	Ь 30	

Некоторые шифровки можно расшифровать несколькими способами. Например, 12112 может означать «АБАК», может — «КАК», а может — «АБААБ». Даны четыре шифровки:

20335 21120 31321 51201

Только одна из них расшифровывается единственным способом. Найдите её и расшифруйте. То, что получилось, запишите в качестве ответа.

Задание 2.

1.Для кодирования букв А, Б, В, Г решили использовать двухразрядные последовательные двоичные числа (от 00 до 11 соответственно). Если таким способом закодировать последовательность символов ГБАВ и записать результат в шестнадцатеричной системе счисления, то получится: 1) 132_{16} 2) $D2_{16}$ 3) 3102_{16} 4) $2D_{16}$

2. Для кодирования букв А, Б, В, Г решили использовать двухразрядные последовательные двоичные числа (от 00 до 11 соответственно). Если таким способом закодировать последовательность символов ГБВА и записать результат шестнадцатеричным кодом, то получится:

a	b	c	d	e
000	110	01	001	10

1) 138_{16} 2) $DBCA_{16}$ 3) $D8_{16}$ 4) 3120_{16}

3. Для 5 букв латинского алфавита заданы их двоичные коды (для некоторых букв - из двух бит, для некоторых - из трех). Эти коды представлены в таблице:

a	b	c	d	e
100	110	011	01	10

Определите, какой набор букв закодирован двоичной строкой 1100000100110

1) baade 2) badde 3) bacde 4) bacdb

4. Для 5 букв латинского алфавита заданы их двоичные коды (для некоторых букв – из двух бит, для некоторых – из трех). Эти коды представлены в таблице:

Определите, какой набор букв закодирован двоичной строкой 1000110110110, если известно, что все буквы в последовательности – разные:

A	B	C	D	E
000	01	100	10	011

1) cbade 2) acdeb 3) acbed 4) bacde

5. Для 5 букв латинского алфавита заданы их двоичные коды (для некоторых букв из двух бит, для некоторых из трех). Эти коды представлены в таблице.

A	B	C	D	E		F
00	100	10	011	11		101

Определить, какой набор букв закодирован двоичной строкой 01 10 100 011 000 1) EBCEA 2)BDCEA 3) BDDEA 4) EBAEA ?

6. Для 6 букв латинского алфавита заданы их двоичные коды (для некоторых букв из двух бит, для некоторых – из трех). Эти коды представлены в таблице:

Определите, какая последовательность из 6 букв закодирована двоичной строкой 011111000101100. 1) DEFBAC 2) ABDEFC 3) DECAFB 4) EFCABD

7. Для кодирования букв A, B, C, D используются трехразрядные последовательные двоичные числа, начинающиеся с 1 (от 100 до 111 соответственно). Если таким способом закодировать последовательность символов CDAB и записать результат в шестнадцатеричном коде, то получится:1) $A52_{16}$ 2) $4C8_{16}$ 3) $15D_{16}$ 4) $DE5_{16}$

8. Для кодирования букв А, Б, В, Г используются четырехразрядные последовательные двоичные числа от 1000 до 1011 соответственно. Если таким способом закодировать последовательность символов БГАВ и записать результат в восьмеричном коде, то получится:

1) 175423 2) 115612 3) 62577 4) 12376

Примеры тестов

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Примеры готовых практических работ:

Практическая работа: Шифрование

Теоретические сведения

— обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Пользователи являются авторизованными, если они обладают определенным аутентичным ключем. Вся сложность и задача шифрования состоит в том, как именно реализован этот процесс.

Шифрование состоит из двух составляющих- зашифровывание и расшифровывание.

С помощью шифрования обеспечиваются три состояния безопасности информации.

1. конфиденциальность (шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении)
2. целостность (шифрование используется для предотвращения изменения информации при передаче или хранении)
3. целостность (шифрование используется для предотвращения изменения информации при передаче или хранении)

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Эти алгоритмы применяются к данным с использованием ключа. Ключи для шифрования и для расшифровывания могут различаться, а могут быть одинаковыми.

Будем называть исходный текст открытым текстом, а результат его шифрования - шифротекстом.

Ключ — это секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности (подлинности).

Шифр цезаря - также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера.

Пример:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Задачи

1. Расшифруйте латинскую пословицу, зная, что она зашифрована шифром Цезаря с ключом 5 (пробелы и запятые - остаются без изменений):

XN ANX UFHJR, UFWF GJQQZR

Важно !!! Ответ должен быть в том же регистре, что и вопрос. Если исходный текст "большими" буквами, то и ответ "большими", если "маленькими", то и ответ "маленькими". И так во всех задачах

Алфавит представлен таблицей:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2. Расшифруйте сообщение с ключом 3

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб

3. Расшифруйте сообщение с ключом 3

Лжзх дюъсн, нгъгзхфв,

Екжюшгзх рг шсжц:

– сш, жсфнг нсръгзхфв,

Фзмъгф г цтгжц!

4. Г ОЦЪЫЗ ЖГЕГМ РГСДСУСХ - 8 ТЛУСЁСЕ Л СЖРГ ФЕЗЪНГ. (ключ 3, шифр Цезаря)

5. ключ 7

ФЖ ЦТЖФЛЩЛ СХФШЛЧИФВЬ ЗЖФХС ЗЖФСП ЦХКЧЖТПШГ Ш ЩЪЯМФСХР!

(от др.-греч. κρυπτός «скрытый» + «анализ») — наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

1. ЪЗХЮУЗ ТОБФ ЖЕГ
2. ЦПЙЫМ. ГЯЯЫККНТ РУТНЖУГШНЙГКЫТ.
3. ВИДРЖ. АИИРЪЪЬК ЮАКЬВААОЬДАЪРК.
4. Вю, й ьцёгю ъюгпх ныщч!
5. Шылкунас цотсацгит юпый

Чошомис оп о кмуце.
Оп цотафышас л кмищупы:
– Пухеп кмуц шлечца, шефце!
Пар шесик кмуцикля втоса,
Угик экору окмяц…

– Ноцпири щурахту л носа –
Тмитпус тко-ко иф мещяк.
По кук цотсацгит ромбикля:
– Па эко елкь ущомбида!

6. Однажды Гай Юлий Цезарь путешествовал на остров Родос. Во время плавания он был захвачен пиратами. Цезарь отправил домой записку, в которой зашифровал сумму выкупа в золотых талантах (1 золотой талант - примерно 26 кг золота):
ТВХЯЖЗФВХ ХГОГРХСЕ

Сколько денег в талантах запросили пираты?

7. пгхзпгхлнц фозжцзх лкцъгхя кгхзп, ъхс срг цп е тсувжсн тулесжлх.

8. Гай Юлий Цезарь зашифровал число восставших гладиаторов. Потом, для надежности, переписал шифровку задом наперед.

ЪВФЮХ ХВФЗЖЯПЗФСЕ

Сколько было гладиаторов?