

Общественная организация «Чувашское региональное отделение
Академии информатизации образования»

УТВЕРЖДАЮ
Председатель научного совета ОО ЧРО АИО
_____ Н.В. Софронова
« _____ » _____ 2016 г.

**Дополнительная профессиональная образовательная программа
повышения квалификации**

«Информационная безопасность»

Форма обучения
дистанционная

Чебоксары 2016 г.

Дополнительная профессиональная образовательная программа повышения квалификации составлена в соответствии с требованиями Федерального закона от 29.12.2012 N 273-ФЗ (ред. от 13.07.2015) "Об образовании в Российской Федерации" и Приказом Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. N 499 г. Москва

Дополнительная профессиональная образовательная программа повышения квалификации «Решение нестандартных задач по информатике» предназначена для повышения квалификации учителей информатики, учителей начальных классов, преподающих информатику, заместителей директоров школ по информатизации, методистов по информатике и других работников образования, ведущие работу с одаренными детьми в области информатики (в дальнейшем слушателей).

Составитель программы: _____ к.п.н., доцент Ю.Н. Егорова

Содержание

1. Цели освоения программы **Ошибка! Закладка не определена.**
2. Требования к результатам освоения программы **Ошибка! Закладка не определена.**
3. Объем программы и виды учебной работы **Ошибка! Закладка не определена.**
4. Содержание программы **Ошибка! Закладка не определена.**
5. Учебно-методическое и информационное обеспечение программы **Ошибка! Закладка не определена.**

1. Цели реализации программы

Целью дополнительной профессиональной образовательной программы повышения квалификации «**Информационная безопасность**» является изучение программно-аппаратных средств защиты информации.

Основными задачами программы являются:

- усвоение методов анализа и планирования информационной защиты компьютерных систем, сетей и их компонентов, средств защиты сетевых служб;
- получение представлений о перспективных направлениях в области защиты информации.

2. Планируемые результаты обучения

В результате освоения программы слушатель будет:

- Знать: положения основных нормативных документов, регламентирующих деятельность основных нормативных документов, регламентирующих деятельность в области защиты информации; основы информационной безопасности; математические основы криптографических методов защиты информации; наиболее распространенные криптографические алгоритмы; основные уязвимости, возникающие при защите компьютерных систем и факторы, влияющие на уровень защищенности; основные подходы к выявлению и предотвращению компьютерных атак.
- Уметь: исследовать криптографические алгоритмы на стойкость, оценивать угрозы защищаемой информации, организовывать защиту информации на объектах ее обработки.
- Владеть: навыками построения и программной реализации алгоритмов шифрования и криптографических систем, навыками оценки уровня защищенности компьютерных систем.

3. Учебный план

Категория слушателей:

учителя информатики, заместители директоров школ по информатизации, методисты по информатике.

Срок обучения: 72 часа

Форма обучения: дистанционная

Режим обучения: по 2 (4) часа в день

Период обучения: 1 (2) месяца

№ раздела	Наименование тем	Всего, (час)	виды учебной работы			
			ЛК	ПР	ЛБ работы	Сам работа
1	2	3	4	5	6	7
1.	Информационная безопасность и уровни ее обеспечения	18	6	-	8	4
2.	Компьютерные вирусы и защита от них	18	6		8	4
3.	Особенности обеспечения информационной безопасности в компьютерных сетях	18	6	-	8	4
4.	Механизмы обеспечения "информационной безопасности"	18	6	-	8	4
	ВСЕГО	72	24		32	16

4. Календарный учебный график

Время освоения курса составляет 72 часа (или 2 зачетных единицы). Изучение курса происходит по следующему графику.

Недели	ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС	В неделю
1	2	2	2	2	2	4	4	18

2	2	2	2	2	2	4	4	18
3	2	2	2	2	2	4	4	18
4	2	2	2	2	2	4	4	18

5. Рабочая программа

№ раздела	Наименование раздела	Содержание раздела программы	Форма текущего контроля
1	2	3	4
1.	Информационная безопасность и уровни ее обеспечения	Проблема информационной безопасности общества. Составляющие информационной безопасности. Система формирования режима информационной безопасности.	тест, решение задач
2.	Компьютерные вирусы и защита от них	Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.	тест, решение задач
3.	Особенности обеспечения информационной безопасности в компьютерных сетях	Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.	тест, решение задач
4.	Механизмы обеспечения "информационной безопасности"	Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей. Криптография и шифрование. Структура криптосистемы. Классификация систем шифрования данных. Механизм электронной цифровой	тест, решение задач

		подписи. Методы разграничение доступа. Регистрация и аудит. Определение и содержание регистрации и аудита информационных систем. Межсетевое экранирование. Классификация межсетевых экранов. Технология виртуальных частных сетей (VPN). Сущность и содержание технологии виртуальных частных сетей.	
--	--	--	--

5.1. Лабораторный практикум

№ п/п	№ раздела программы	Наименование работ	Трудоемкость
			часы
1	2	3	4
1.	1	Ознакомление с аппаратом программирования на языке Visual Basic for Applications, примерами программ для решения простых задач. Разработка программы выработки пар «открытый/закрытый» ключ по методу RSA. Шифрование конфиденциальных данных.	8
2.	2	Изучение принципов работы линейного сдвигового регистра с обратной связью (ЛПРОС) и организацию шифрования на их основе.	8
3.	3	Разработка клиент-серверного приложения для двустороннего обмена информацией между компьютерами в сети. Выполнение пробной передачи и прием данных. Выработка секретного ключа по протоколу Диффи-Хелмана. Аутентификация пользователей по «слово-вызов».	8
4.	4	Основные алгоритмы аутентификации пользователей в	8

		сети, электронно- цифровой подписи, сертификации. Разработка комплекса программ для пересылки и проверки идентификаторов пользователей, решение задач распределения секретного ключа, идентификации посланий на основе электронно- цифровой подписи и сертификатов.	
--	--	---	--

5.2 Самостоятельная работа слушателей

№ п/п	Содержание раздела	Виды СРС		Объем час	Формы контроля
		обязательные	дополнительные		
1	2	3	4	5	6
1	Информационная безопасность и уровни ее обеспечения	Шифр перестановки «скитала».	Шифры перестановки	4	
2	Компьютерные вирусы и защита от них	Шифрующие таблицы.	Шифры простой замены.	4	
3	Особенности обеспечения информационной безопасности в компьютерных сетях	Применение магических квадратов.	Полибианский квадрат.	4	
4	Механизмы обеспечения "информационной безопасности"	Шифры простой замены.	Система шифрования Цезаря.	4	

6. Оценочные материалы

Примерные вопросы на зачет

- Происхождение термина «криптография»:
 - от слова «тайнопись»;
 - от слова «шифрование»;
 - от термина «скремблирование»;
 - от термина «кодирование».
- Метод надежной передачи информации по открытому каналу связи использует:
 - криптографию;

- б) стеганографию;
 - в) кодирование;
 - г) скремблирование.
3. Для чего используется система Kerberos?
- а) для симметричной аутентификации;
 - б) для несимметричной аутентификации;
 - в) для выработки ЭЦП;
 - г) для шифрования.
4. Что такое код обнаружения манипуляции с данными MDC?
- а) есть результат действия хэш-функции;
 - б) циклический контрольный код сообщения;
 - в) код четности;
 - г) имитоприставка.
5. Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:
- а) ЭЦП;
 - б) криптография;
 - в) криптоанализ;
 - г) стеганография.
6. Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:
- а) простейшим шифром;
 - б) блочным шифром;
 - в) шифром подстановки;
 - г) шифром замены.
7. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:
- а) линейные функции;
 - б) нелинейные функции;
 - в) односторонние функции;
 - г) функции преобразования.
8. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:
- а) гибридные криптосистемы;
 - б) криптосистема RSA;
 - в) электронная подпись;
 - г) криптографические протоколы.
9. Как называют в ГОСТе режим электронной кодовой книги (ECB):
- а) режим сцепления блоков шифротекста;
 - б) режим простой замены;
 - в) режим обратных связей по выбору;

- г) режим счетчика.
10. Процесс применения шифра защищаемой информации называют:
- а) дешифрованием;
 - б) вскрытием шифра;
 - в) простой заменой;
 - г) шифрованием.
11. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:
- а) ключ;
 - б) разрядность блока;
 - в) число раундов шифрования;
 - г) алгоритм шифрования.
12. Процесс наложения по определенному закону гамма-шифра на открытые данные:
- а) хэширование;
 - б) имитовставка;
 - в) гаммирование;
 - г) ЭЦП.
13. Чему равна разрядность блока алгоритма шифрования DES:
- а) 56 битам;
 - б) 128 битам;
 - в) 64 битам;
 - г) 256 битам.
14. Разрядность 3DES равна:
- а) 56 бит;
 - б) 112 бит;
 - в) 168 бит;
 - г) 256 бит.
15. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:
- а) простыми криптосистемами;
 - б) гибридными криптосистемами;
 - в) ассиметричными криптосистемами;
 - г) симметричными криптосистемами.

7. Формы аттестации

Итоговый контроль осуществляется в рейтинговой форме с учетом изучения слушателем всего лекционного материала выполнения лабораторных работ, активности в ходе прохождения программы, прохождением теста по разделам курса и защиты проекта.

- 10 баллов – выполнение одной лабораторной работы;

- 10 баллов – выполнение одного теста;

Итого: Рейтинг = (10 баллов * 4 лаб. работ) + (10 баллов * 6 тестов) = 40 баллов + 60 баллов = 100 баллов.

Оценка	Критерии оценки степени сформированности компетенций
Зачтено	Выполненное задание, посещаемость более 60%
Не зачтено	Не выполнено задание, посещаемость менее 60%

8. Организационно-педагогические условия

8.1 Учебная литература и другие информационные источники

1. Алешников С. И. Математические методы защиты информации: учебное пособие / Алешников С. И., Пышкин А. В. - Калининград: Изд-во КГУ, 2003. - 119с.. - ISBN 5-88874-439-5.
2. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии: МЦНМО / Василенко О. Н., Ин-т пробл. информ. безопасности МГУ - М.: МЦНМО, 2003. - 325с. - (Информационная безопасность криптографии). - ISBN 5-94057-103-4.
3. Введение в криптографию. Яценко В. В., Варновский Н. П., Нестеренко Ю. В. и др. ; под ред. Яценко В. В. - СПб. [и др.]: МЦНМО, Питер, 2001. - 287с. - (Новые математические дисциплины). - ISBN 5-318-00443-1.
4. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах: Изд-во Урал. ун-та / Гайдамакин Н. А. - Екатеринбург: Изд-во Урал. ун-та, 2003. - 327с.. - ISBN 5-86037-024-5.

8.2. Дополнительная литература:

5. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Учебный курс. М.: Горячая линия.–Телеком, 2001
6. Брэгг Р. Безопасность сети на основе Microsoft Windows Server 2003. Учебный курс Microsoft / Пер. с англ. – М.: Издательский дом "Русская редакция", СПб.: "Питер", 2006.
7. Бузов Г.А. и др. Защита от утечки информации по техническим каналам. – М.:Телеком,2005

8.3 Образовательные технологии

Интерактивные образовательные технологии, используемые в обучении.

1. Вебинары на базе системы BigBlueButton <http://bigbluebutton.infoznaika.ru/>
2. СДО Moodle <http://moodle.infoznaika.ru/>

