Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана» (национальный исследовательский университет)
(МГТУ им. Н. Э. Баумана)

УТВЕРЖДАЮ
Первый проректор-проректор по учебной работе
МГТУ им. Н.Э. Баумана
_____ Б.В. Падалкин
«25» ____09____ 2016 г.

ПРОГРАММА

КУРСОВОГО ЦИКЛА ПО ВЫБОРУ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЦИКЛ ЗАНЯТИЙ
«ВВЕДЕНИЕ В ИНЖЕНЕРНУЮ СПЕЦИАЛЬНОСТЬ. БАУМАНСКАЯ ШКОЛА БУДУЩИХ ИНЖЕНЕРОВ»
для учащихся профильных инженерных классов московских школ

Автор(ы): Астрахов Алексей Витальевич, к.т.н., доцент,
Зеленцова Екатерина Валентиновна, к.т.н., доцент

Москва, 2016 г.

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Программа выполнена в рамках образовательного проекта Департамента образования города Москвы «Инженерный класс в московской школе». Программа направлена на внедрение новых форм и методов обучения, его индивидуализацию, использование комплекса новейших технических средств и технологий обучения с акцентом на активные виды самостоятельной индивидуальной работы. Актуальность программы связана с необходимостью реагировать на современные вызовы и социально-экономические изменения, происходящие в мире и обществе, связанные с потребностью в новых профессиональных качествах современных специалистов: способностью быстро адаптироваться к меняющимся условиям трудовой деятельности, самообразовываться и саморазвиваться, оптимизировать энергозатраты, эффективно использовать имеющиеся ресурсы и др. Программа соответствует приоритетному направлению развития науки, технологий и техники в Российской Федерации (утв. Указом Президента РФ от 7 июля 2011 г. N 899) «Информационно-телекоммуникационные технологии» и направлена на получение знаний, умений и навыков в области создания комплексной системы обеспечения информационной безопасности разнородных инфокоммуникационных структур. Педагогическая целесообразность проекта обусловлена расширением традиционной дидактической парадигмы, ориентированной на репродуктивное обучение, наполнение ее элементами проектного инженерного образования. Отличительной особенностью программы является формирование сопряжённых между собой индивидуализированных образовательных траекторий школьников, реализуемых в рамках единой тематики проекта. Программа ориентирована на учащихся 8-11 классов школы и состоит из четырех взаимосвязанных этапов длительностью три академических часа каждый, требующих поочередного прохождения обучения. Ожидаемыми результатами реализации проекта на уровне учащегося является активизация мыслительной активности, укрепление межпредметных связей, формирование критического и творческого мышления, повышение мотивации к получению инженерного образований и др. Результаты освоения полученных знаний, умений и навыков будут оценены и проверены с помощью бипарадигмальной методологии, основанной на получение количественных данных тестирования и качественных экспертных оценок, что гарантирует получение объективной информации о фактическом уровне учебных достижений.

Ключевые слова: профильное инженерно-техническое обучение, учащиеся инженерных классов московских школ, профильное инженерно-техническое обучение, мотивация к получению инженерной профессии, индивидуальный проект, научно-методическая и организационная поддержка проекта «Инженерный класс в московской школе», практико-ориентированное обучение, экспериментальное исследование на кафедрах и в лабораториях, деятельностно-компетентностный подход к обучению школьников, взаимодействие с профессорско-преподавательским составом Университета, интеграция лекций, практических занятий и проектно-исследовательской деятельности, получение и анализ полученных результатов, коллоквиум, метапредметные связи, формирование компетенций школьников в области информационной безопасности, развитие познавательных интересов.

1.2. Категория обучающихся: учащиеся 8-11 классов образовательных организаций города Москвы, осуществляющих профильное инженерно-техническое обучение.

1.3. Цель программы состоит в создании базовых условий и формировании предпосылок, при которых учащиеся профильных инженерных классов будут самостоятельно и при консультативно-информационной поддержке преподавателей университета приобретать недостающие знания из разных областей науки и техники; пользоваться и закреплять приобретенные ранее знания при решении практических задач; приобретать коммуникативные навыки при работе в малых рабочих группах; развивать системное мышление, творческие способности и исследовательские умения.

1.4. Задачи программы

- оказывать содействие развитию творческих способностей и интеллекта учащегося;
- погружать учащегося в логику профессиональной деятельности, повышая его мотивацию в получении необходимых для этого знаний, умений и навыков;
- сформировать, корректировать и контролировать содержание, структуру и темп реализации индивидуального плана работы над проектом;
- обеспечить комплексный подход к получению искомых результатов проекта, дозированное и сбалансированное предоставление новой информации и практических материалов, обеспечивая комфортные условия для физиологического и психического состояния ученика;
- создать условия для осознанного усвоение новых знаний на примере их использования в решении прикладных инженерно-технических задач в области информационной безопасности и обучить учащихся получать знания через практическую деятельность.

1.5 Трудоемкость обучения:

- срок обучения – 12 аудиторных часов, 4 недели;
- из них контролируемая самостоятельная работа обучающихся под руководством профессорско-преподавательского состава МГТУ им. Н.Э.Баумана – 4 аудиторных часа.

1.6. Режим занятий – 3 аудиторных часа в день, 1 раз в неделю, октябрь-ноябрь.

1.7. Форма обучения – очная, без отрыва от занятий.

II. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ

Обучающийся, освоивший программу, должен:

2.1. Знать: основы научного стиля мышления и инженерной деятельности; последовательность и сущность умственно-практических действий, принципы формирования алгоритмических и эвристических приемов умственной деятельности при решении задач информационной безопасности.

2.2. Уметь:

- планировать и проводить этапы исследования;
- контролировать, систематизировать, анализировать и обобщать результаты практических занятий;
- формулировать гипотезу исследования и структурировать этапы выполнения индивидуального задания по проекту;
- организовать и контролировать физиологическую и психическую деятельность;
- представлять и защищать результаты выполнения индивидуального задания;
- творчески мыслить и переносить имеющиеся знания на текущее поле деятельности;
- критически оценивать результаты собственной исследовательской работы;
- использовать различные открытые источники информации, работать с литературой, осознанно воспринимать и анализировать собранные данные для достижения поставленных целей научно-творческой деятельности;

2.3. Приобрести навыки: самостоятельной индивидуальной, групповой и коллективной работы над проектом; актуализации собственного имеющегося опыта; субъект-субъектных от-

ношений и диалогового межличностного общения, сотрудничества и сотворчества,

2.5. Формы подведения итогов реализации дополнительной образовательной программы: коллоквиум с защитой индивидуального проекта, блиц-опрос, результаты текущего рубежного контроля.

III. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Учебный план

№ п/п	Виды занятий	Объем занятий (час.)
1.	Научные лекции	4
2.	Практические занятия в лабораториях кафедры «Защита информации» (ИУ-10) МГТУ им. Н.Э. Баумана	4
3.	Выполнение проектно-исследовательской работы	3
4.	Итоговое мероприятие - коллоквиум	1
ВСЕГО		12

3.2. Тематический учебный план

№ п/п	Наименование темы	Всего часов	В том числе:			Форма контроля
			Лекции*	Научный практикум**	Выполнение проектно-исследовательской работы	
1.	Информационная безопасность в контексте национальной безопасности Российской Федерации	3	1	1	1	-
2.	Эволюция угроз информационной безопасности.	3	1	1	1	Блиц опрос
3.	Управление информационными рисками.	3	1	1	1	-
4.	Основы информационно-психологической безопасности	2	1	1		Рубежный контроль
5.	Итоговое мероприятие - коллоквиум	1			1	Защита проекта
ВСЕГО		12	4	4	4	

** - изучение теоретических зависимостей и их прикладных свойств по тематике цикла*
*** - научный практикум может включать семинарские занятия, деловые и ролевые игры с моделированием изучаемых процессов, работу на современном лабораторном оборудовании*

3.3. Учебная программа

№ п/п	Темы лекций, практических занятий, исследовательских проектов учащихся	Содержание лекций, практических занятий, исследовательских проектов учащихся, используемых образовательных технологий и заданий для контролируемой самостоятельной работы обучающихся; перечень рекомендуемой литературы
	Название темы (12 часов)	
1.	*Лекция 1. (1 час)*	Информационная безопасность в контексте национальной безопасности Российской Федерации.
2.	*Практическое занятие 1. (1 час)*	Практическое изучение основ криптографической защиты информации. Шифр Цезаря. «Отзеркаливание» алфавита. Квадрат Полибия. Шифр Аббата Тримемиуса.
3.	*Выполнение проектно-исследовательской работы (1 час)*	Работа школьников идет в командах, объединенных близкой темой. Используется проектный подход к обучению. Школьники выполняют следующие виды работ: • анализ литературы по вопросам защиты информации. • изучение технических характеристик конкретного программного продукта и его возможностей, • получение индивидуальных консультаций.
4.	*Лекция 2. (1 час)*	Эволюция угроз информационной безопасности.
5.	*Практическое занятие 2. (1 час)*	Создание виртуального полигона и базовой инфраструктуры для проведения экспериментов в области безопасности компьютерных сетей.
6.	*Выполнение проектно-исследовательской работы (1 час))*	Работа школьников идет в командах, объединенных близкой темой. Используется проектный подход к обучению. Школьники выполняют следующие виды работ: • анализ литературы по вопросам защиты информации. • изучение технических характеристик конкретного программного продукта и его возможностей, • получение индивидуальных консультаций.
7.	*Лекция 3. (1 час)*	Управление информационными рисками.
8.	*Практическое занятие 3. (1 час)*	Знакомство с набором инструментов тестирования безопасности дистрибутива Kali Linux.
9.	*Выполнение проектно-исследовательской работы (1 час)*	Работа школьников идет в командах, объединенных близкой темой. Используется проектный подход к обучению. Школьники выполняют следующие виды работ: • анализ литературы по вопросам защиты информации. • изучение технических характеристик конкретного программного продукта и его возможностей, • получение индивидуальных консультаций.
10.	*Лекция 4. (1 час)*	Основы информационно-психологической безопасности.

11.	*Практическое занятие 4. (1 час)*	Знакомство с принципами работы полиграфа
12.	*Итоговое мероприятие - коллоквиум*	*Содержание коллоквиума (с обсуждением полученных результатов и защитой проектов)*

3.4. Список тем исследовательских проектов

№ п/п	Название темы	Краткая аннотация проекта (*цели, задачи, методы исследования*)
1.	Исследование принципов работы Антивируса Касперского для Windows	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Касперского для Windows **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
2.	Исследование систем анализа уязвимостей на основе пакета MetasploitFraimwork	**Цель** – Исследование принципов работы систем анализа уязвимостей на примере MetasploitFraimwork **Задачи:** 1.Изучение литературы в области систем анализа уязвимостей. 2.Изучение архитектуры MetasploitFraimwork. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы MetasploitFraimwork. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
3	Исследование систем обнаружения вторжений на примере SNORT для LINUX	**Цель** – Исследование принципов работы систем обнаружения вторжений на примере SNORT **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры SNORT. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы SNORT. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.

4	Исследование принципов работы снифферов пакетов на примере WireShark	**Цель** – Исследование принципов работы снифферов пакетов на примере WireShark **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры WireShark. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы WireShark. **Методы исследования:** анализ литературы в области защиты информации. изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
5	Исследование принципов работы межсетевых экранов на примере IPTABLES для LINUX	**Цель** – Исследование принципов работы межсетевых экранов на примере IPTABLES **Задачи:** 1.Изучение литературы в области межсетевых экранов. 2.Изучение архитектуры IPTABLES. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы IPTABLES. **Методы исследования:** анализ литературы в области защиты информации. изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
6	Исследование принципов работы Антивируса AVG Anti-Virus Free	**Цель** – Исследование принципов работы СЗИ на примере Антивируса AVG Anti-Virus Free. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
7	Исследование принципов работы Антивируса Avast! AntivirusHome для Windows	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Avast! AntivirusHome для Windows. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ

		Методы исследования: анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
8	Исследование принципов работы межсетевых экранов на примере Comodo Personal Firewall для ОС Windows	**Цель** – Исследование принципов работы межсетевых экранов на примере Comodo Personal Firewall **Задачи:** 1.Изучение литературы в области межсетевых экранов. 2.Изучение архитектуры Comodo Personal Firewall. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы Comodo Personal Firewall. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
9	Исследование систем обнаружения вторжений на примере Bro NIDS для LINUX	**Цель** – Исследование принципов работы систем обнаружения вторжений на примере Bro NIDS **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры Bro NIDS. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы Bro NIDS. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
10	Исследование принципов работы Антивируса AviraAntiVirPersonal – FreeAntivirus	**Цель** – Исследование принципов работы СЗИ на примере Антивируса AviraAntiVirPersonal – FreeAntivirus. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
11	Исследование принципов работы межсетевых экранов	**Цель** – Исследование принципов работы межсетевых экранов на примере Ashampoo Firewall Free **Задачи:**

	на примере Ashampoo Firewall Free	1.Изучение литературы в области межсетевых экранов. 2.Изучение архитектуры Ashampoo Firewall Free . 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы Ashampoo Firewall Free . **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
12	Исследование принципов работы межсетевых экранов на примере PC Tools Firewall Plus	**Цель** – Исследование принципов работы межсетевых экранов на примере PC Tools Firewall Plus. **Задачи:** 1.Изучение литературы в области межсетевых экранов. 2.Изучение архитектуры PC Tools Firewall Plus. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы PC Tools Firewall Plus. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
13	Исследование принципов работы Антивируса Dr Web	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Dr Web. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
14	Исследование принципов работы Антивируса Panda Cloud Antvirus Free	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Panda Cloud Antvirus Free. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения,

		изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
15	Исследование принципов работы снифферов пакетов на примере SmartSniff	**Цель** – Исследование принципов работы снифферов пакетов на примере SmartSniff **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры SmartSniff. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы SmartSniff. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
16	Исследование принципов работы снифферов пакетов на примере IP Sniffer	**Цель** – Исследование принципов работы снифферов пакетов на примере IP Sniffer **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры IP Sniffer. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы IP Sniffer. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
17	Исследование систем анализа уязвимостей на основе пакета Microsoft Baseline Security Analyzer	**Цель** – Исследование принципов работы систем анализа уязвимостей на примере Microsoft Baseline Security Analyzer **Задачи:** 1.Изучение литературы в области систем анализа уязвимостей. 2.Изучение архитектуры Microsoft Baseline Security Analyzer. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы Microsoft Baseline Security Analyzer . **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
18	Исследование систем анализа уязвимостей на основе пакета OpenVAS	**Цель** – Исследование принципов работы систем анализа уязвимостей на примере OpenVAS **Задачи:** 1.Изучение литературы в области систем анализа уязвимостей. 2.Изучение архитектуры OpenVAS. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы OpenVAS .

		Методы исследования: анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
19	Исследование систем анализа уязвимостей на основе пакета SurfPatrol	**Цель** – Исследование принципов работы систем анализа уязвимостей на примере SurfPatrol **Задачи:** 1.Изучение литературы в области систем анализа уязвимостей. 2.Изучение архитектуры SurfPatrol. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы SurfPatrol . **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
20	Исследование принципов работы Антивируса PC Tools AntiVirus Free Edition	**Цель** – Исследование принципов работы СЗИ на примере Антивируса PC Tools AntiVirus Free Edition **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
21	Исследование принципов работы Антивируса Microsoft Malicious Removal Tool для Windows	**Цель** – Исследование принципов работы СЗИ на примере Microsoft Malicious Removal Tool для Windows **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
22	Исследование принципов работы	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Norton Internet Security

	Антивируса Norton Internet Security	**Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
23	Исследование систем обнаружения вторжений на примере OSSEC для LINUX	**Цель** – Исследование принципов работы систем обнаружения вторжений на примере OSSEC для LINUX **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры OSSEC для LINUX. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы OSSEC для LINUX. **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
24	Исследование систем обнаружения вторжений на примере OSSEC для WINDOWS	**Цель** – Исследование принципов работы систем обнаружения вторжений на примере OSSEC для WINDOWS. **Задачи:** 1.Изучение литературы в области систем обнаружения вторжений. 2.Изучение архитектуры OSSEC для WINDOWS. 3.Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы OSSEC для WINDOWS/ **Методы исследования:** анализ литературы в области защиты информации, изучение технических характеристик конкретного программного продукта и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
25	Исследование принципов работы Антивируса Comodo AntiVirus	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Comodo AntiVirus. **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности

		работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
26	Исследование принципов работы Антивируса Microsoft Security Essentials	**Цель** – Исследование принципов работы СЗИ на примере Антивируса Microsoft Security Essentials **Задачи:** 1. Изучение литературы в области антивирусного ПО. 2. Изучение архитектуры заданного СЗИ. 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы конкретного СЗИ. 4. Проведение эксперимента для оценки эффективности работы СЗИ **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик конкретного СЗИ и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
27	Исследование принципов работы программы CrypTool.	**Цель** – Исследование принципов криптографической защиты информации на основе программы CrypTool **Задачи:** 1. Изучение литературы в области основ криптографии. 2. Изучение архитектуры программы CrypTool 3. Проведение экспериментов с помощью программы CrypTool **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик ПО и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
28	Исследование принципов работы программы PGP.	**Цель** – Исследование принципов криптографической защиты информации на основе программы PGP **Задачи:** 1. Изучение литературы в области основ криптографии. 2. Изучение архитектуры программы PGP. 3. Проведение экспериментов с помощью программы PGP. **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик ПО и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
29	Исследование архитектуры и принципов работы программы sshd для Linux	**Цель** – Исследование принципов работы алгоритмов с открытым ключем на примере программы sshd для Linux **Задачи:** 1. Изучение литературы в области основ криптографии. 2. Изучение архитектуры программы sshd для Linux 3. Разработка стенда на основе виртуальных машин для проведения экспериментальной проверки работы

		конкретного СЗИ. 4. Проведение экспериментов с помощью sshd для Linux **Методы исследования:** анализ литературы по вопросам антивирусного обеспечения, изучение технических характеристик ПО и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.
30	Речевые технологии: области применения, современное состояние и перспективы развития.	**Цель** – Анализ основных направлений исследований в области речевых технологий и перспектив их развития. 1. Изучение литературы в области речевых технологий. 2. Изучение программного обеспечения на основе речевых технологий. 3. Перспективы разработки систем распознавания речи. **Методы исследования:** анализ литературы по вопросам существующих речевых технологий, изучение технических характеристик ПО и его возможностей, получение индивидуальных консультаций преподавателей Университета – ведущих специалистов по защите информации.

3.5. Самостоятельная работа школьников

Задание по формированию и развитию инновационно-творческой компетенции учащихся инженерных классов	Практическое выполнение слушателями учебно-исследовательских работ под руководством преподавателей Университета
Задание по развитию экспериментально-исследовательской компетенции учащихся инженерных классов	Практическое занятие по освоению навыков принятия и обработки экспериментальных данных, полученных на лабораторном оборудовании МГТУ им. Н.Э.Баумана с применением новейших программных продуктов.

3.6. Рекомендуемая литература

1.	Основная	1. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. Под. ред. В.А. Садовничего и В.П. Шерстюка. - М., 2004. 2. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с., ил. 3. Полиграф в России. 1993-2008: Ретроспектив. сб. науч. ст., посвящен. 15-летию применения полиграфа в РФ / авт.-сост. Холодный Ю. И. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2008. - 176 с. - Библиогр.: с. 170-176.
2.	Дополнительная	4. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа, М: РадиоСофт, 2010. – 232 с. 5. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999. - 108с.
3.	Электронные ресурсы	6. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне [Электронный ресурс] : электронное учебное издание : учебное пособие по дисциплине "Противодействие компьютерным атакам" / Климов С. М., Сычев М. П., Астрахов А. В.; МГТУ им. Н. Э. Баумана, Фак. "Информатика и системы управления", Каф. "Защита информации". - Москва : МГТУ им. Н. Э. Баумана, 2013. - 1 электрон. опт. диск (CD-ROM); 12 см. Загл. с этикетки диска// http://wwwedl.bmstu.ru/iu10/comp-atak-exp.htm

IV. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

4.1. Итоговое мероприятие

При реализации программы применяется следующая форма педагогического контроля обучающихся: блиц опрос, рубежный контроль. Итоговый контроль – коллоквиум с обсуждением результатов и защитой индивидуальных проектов.

V. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

5.1. Материально-технические условия реализации программы

Материально-техническая база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов учебных занятий.

Аудиторный фонд, где будут проводиться занятия оборудован всеми необходимыми техническими средствами обучения. Материально-техническое обеспечение занятий включает наличие компьютерной базы с выходом в Интернет, мультимедийные проекторы, кодоскопы, кино-, теле- и аудиоаппаратуру, а также лабораторно-экспериментальное оборудование кафедры «Защита информации» (ИУ-10) МГТУ им. Н.Э. Баумана.

5.2. Квалификация преподавателей, участвующих в реализации программы

В разработке и выполнении программы участвуют кадры высшей квалификации, имеющие соответствующие ученые и почетные звания, а также большой научно-педагогический опыт в области подготовки специалистов по информационной и информационно-психологической безопасности.

Астрахов Алексей Витальевич – кандидат технических наук, доцент кафедры «Защита информации»,

Зеленцова Екатерина Валентиновна – кандидат технических наук, доцент кафедры «Защита информации»,

Козлачков Сергей Борисович – кандидат технических наук, доцент кафедры «Защита информации».

Автор(ы) программы:

_____ Астрахов А.В., к.т. н., доц.
подпись *расшифровка подписи автора*

_____ Зеленцова Е.В., к.т.н., доц.
подпись *расшифровка подписи автора*

СОГЛАСОВАНО:

Руководитель
научно-образовательного коллектива
Мероприятия № 8,
Начальник отдела взаимодействия с профильными школами
Центра довузовской подготовки
МГТУ им. Н.Э. Баумана, к.т.н., доц. _____ Н.Ф. Зеленцова
подпись *расшифровка подписи*

«07» 09 2016 г.