МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра математики и физики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» декабря 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б1.В.ДВ.09.01

НАПРАВЛЕНИЕ ПОДГОТОВКИ

01.03.02 Прикладная математика и информатика

ПРОФИЛЬ ПОДГОТОВКИ

Инженерия программного обеспечения

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся проектному и производственно-технологическому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане. Способствует формированию фундаментальных теоретических знаний в области применения методов защиты информации, комплексного проектирования и анализа защищенных автоматизированных систем.

Цель дисциплины

Освоение студентами принципов и методов защиты информации, комплексного проектирования и анализа защищенных автоматизированных систем. Развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства и информационной инфраструктуры общества и государства.

Обеспечение бакалавров опорными знаниями для выполнения научно-исследовательских работ и практических работ, связанных с широким набором вопросов защиты информации и организации систем информационной безопасности.

Задачи дисциплины

Сформировать понятия о вопросах:

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- процесса сбора, передачи, накопления и обработки информации;
- методов и средств ведения информационных войн;
- оценки защищенности и обеспечения информационной безопасности объектов информатизации.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОПК-2	способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии	**знать:** – современные образовательные и информационные технологии, информационные системы и ресурсы; **уметь:** – находить, классифицировать и использовать информационные интернет- технологии, базы данных, webресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний; **владеть:** – знаниями в области современных технологий, баз данных, webресурсов, специализированного программного обеспечения и т.п. и их практическим применением;
ПК-5	способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках	**знать**: - различные типы информации, которые можно извлекать из сети Интернет **уметь:** - приобретать новые научные и профессиональные знания, используя современные технологии поиска информации в глобальных компьютерных сетях **владеть**: - навыками осуществлять целенаправленный поиск информации о научных и технологических достижениях в сети Интернет.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.09.01 Теоретические основы информационной безопасности относится к элективной части и является дисциплиной по выбору.

Представляет основу для изучения дисциплин: Программные средства защиты информации, Технические средства и методы защиты информации, Управление информационной безопасностью.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	*Курс*	*Семестр*	*Трудоемкость дисциплины в часах*						*Курсовая работа (проект), контрольная работа, реферат, РГР*	*Вид промежуточной аттестации*
			Всего часов (с экз.)	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Семинары Практические занятия*	*Самостоятельная работа*		
1	2	3	4	5	6	7	8	9	10	11
Очная	3	6	108	51	17	34	-	57	-	зачет
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудоемкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, час*
			6
1	**2**	**3**	**4**
I. Контактная работа обучающихся с преподавателем (всего)	51	6	51
Лекции (Лк)	17	6	17
Лабораторные работы (ЛР)	34	-	34
Групповые (индивидуальные) консультации	+	+	+
II.Самостоятельная работа обучающихся (СР)	57	-	57
Подготовка к лабораторным работам	40	-	40
Подготовка к зачету	17	-	17
III. Промежуточная аттестация зачет	+	-	+
Общая трудоемкость дисциплины час.	108	-	108
зач. ед.	3	-	3

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий - для очной формы обучения:

№ раздела и темы	*Наименование раздела и тема дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*		
			учебные занятия		*самостоятельная работа обучающихся**
			лекции	*лабораторные работы*	
1	**2**	**3**	**4**	**5**	**6**
1.	**Структура теории компьютерной безопасности.**	**43**	**8**	**14**	**21**
1.1.	Основные понятия теории компьютерной безопасности.	18	4	6	8
1.2.	Методология построения защищенных автоматизированных систем.	25	4	8	13
2.	**Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.**	**65**	**9**	**20**	**36**
2.1.	Политика безопасности.	32	4	10	18
2.2.	Стандарты в области информационной безопасности.	33	5	10	18
	ИТОГО	**108**	**17**	**34**	**57**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	*Наименование раздела и темы дисциплины*	*Содержание лекционных занятий*	*Вид занятия в интрактивной, активной, инновационной формах, (час.)*
1	**2**	**3**	**4**
1.	**Структура теории компьютерной безопасности.**		
1.1.	Основные понятия теории компьютерной безопасности.	История развития теории и практики обеспечения компьютерной безопасности. По нятия "информационная безопасность" и компьютерная безопасность. Безопасность ин формации в компьютерных системах и ее составляющие - конфиденциальность, целост ность и правомерная доступность (сохранность) информации. Субъекты и объекты безо пасности. Угрозы безопасности. Нарушители безопасности. Общие принципы обеспечения компьютерной безопасности. Систематика методов и механизмов обеспечения компьютер ной безопасности.	Лекция-беседа (2 часа)
1.2.	Методология построения защищенных автоматизированных систем.	Общая характеристика политики дискреционного доступа. Тройки доступа: субъект- операция-объект. Модели дискреционного (избирательного) разграничения доступа и мо дели распространения прав доступа. Пятимерное пространство Хартсона как пример выра жения	

		дискреционного разграничения доступа на языке реляционной алгебры. Модели раз граничения доступа на основе матрицы доступа. Принудительный и добровольный прин цип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX) и децентрализованная структура (списки доступа объектов в ОС Windows). Построение систем защиты от угрозы нарушения конфиденциальности и целостности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы.	
2.	**Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.**		
2.1.	Политика безопасности.	Основные определения. Угрозы информационной безопасности, их классификация. Разглашение, утечка, несанкционированный доступ к информации. Правила работы с машинными носителями информации. Формальные модели информационной безопасности. Модель политики контроля целостности. Модель Кларка-Вилсона. Идентификация и аутентификация. Виды парольных систем. Угрозы безопасности парольных систем. Атаки на парольные системы. Построение парольных систем.	Разбор конкретных ситуаций (2 часа)
2.2.	Стандарты в области информационной безопасности.	Основы нормативно-правовой ЗИ. Основные нормативные документы РФ по ЗИ. Защита государственной тайны. Защита коммерческой тайны (КТ). Доктрина ИБ РФ. Государственные органы РФ, отвечающие за нормативно-правовое обеспечение ИБ. Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Стандарт оценки безопасности компьютерных систем TCSEC, Гостехкомиссии РФ. Единые критерии безопасности информационных технологий.	Разбор конкретных ситуаций (2 часа)

4.3. Лабораторные работы

№ п/п	*Номер раздела дисциплины*	*Наименование лабораторной работы*	*Объем в часах*	*Вид занятия в инновационной форме*
1.	**1.**	Изучение программных средств защиты от несанкционированного доступа	2	-
2.		Анализ угроз информационной безопасности.	4	-
3.		Реализация систем парольной защиты и их анализ.	4	-
4.		Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра.	4	-
5.	**2.**	Исследование нормативно-правовой базы информационной безопасности предприятия	4	-

6.		Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.	4	-
7.		Причины, виды, каналы утечки и искажения информации.	6	-
8.		Ассиметричные алгоритмы шифрования данных	6	-
		ИТОГО	**34**	**-**

4.4. Практические занятия

учебным планом не предусмотрено.

4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

учебным планом не предусмотрено.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции*		*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ОПК	*ПК*				
		2	*5*				
1	2	3	4	5	6	7	8
1. Структура теории компьютерной безопасности.	43	+	+	2	21,5	Лк, ЛР, СР	зачет
2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	65	+	+	2	32,5	Лк, ЛР, СР	зачет
всего часов	**108**	**54**	**54**	**2**	**54**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие/Ю.Н. Сычев.-М.: Изд. центр ЕАОИ, 2010.-328 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=90790

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	***Вид занятия*** (*Лк, ЛР*)	***Количество экземпляров в библиотеке,*** **шт.**	***Обеспеченность,*** **(экз./ чел.)**
1	2	3	4	5
Основная литература				
1.	Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=438331	*Лк, ЛР,*	1 (ЭУ)	1
2.	Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=362895	*Лк, ЛР,*	1 (ЭУ)	1
3.	Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=363040	*Лк, ЛР,*	1 (ЭУ)	1
Дополнительная литература				
4.	Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	*Лк, ЛР,*	1 (ЭУ)	
5.	Загинайлов Ю.Н. Теория информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=276557	*Лк, ЛР,*	1 (ЭУ)	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе обучения студенты могут использовать общие ресурсы:
1.Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.
2. Электронная библиотека БрГУ
http://ecat.brstu.ru/catalog .
3. Электронно-библиотечная система «Университетская библиотека online»
http://biblioclub.ru .
4. Электронно-библиотечная система «Издательство «Лань»
http://e.lanbook.com .
5. Информационная система "Единое окно доступа к образовательным ресурсам"
http://window.edu.ru .
6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .
7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
https://uisrussia.msu.ru/ .
8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина призвана обеспечить раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности; определения теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации; классификации и характеристики составляющих информационной безопасности и защиты информации; установления взаимосвязи и логической организации входящих в 15 них компонентов:

- ознакомление с понятийным аппаратом в области информационной безопасности и защиты информации;
- рассмотрение базовых содержательных положений в области информационной безопасности и защиты информации;
- изучение современной доктрины информационной безопасности;
- определение целей и принципов защиты информации; установление факторов, влияющих на защиту информации;
- ознакомление с составом защищаемой информации, ее классификацией по видам тайны, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- рассмотрение направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- определение сущности компонентов защиты информации;
- определение назначения, сущности и структуры систем защиты информации.

Программа раскрывает содержание курса, определяет последовательность усвоения знаний и структуру смысловых связей в рамках изучаемого предмета.

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1 Изучение программных средств защиты от несанкционированного доступа.

Цель работы: Изучить основные программные средства защиты от несанкционированного доступа; определить политику безопасности системы.

Задание:

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра.

2. Включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE).

3. Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра (если лабораторная работа выполняется в операционной системе Windows).

4. Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

Порядок выполнения:

Работа с реестром в Windows

Раздел HKEY_CURRENT_USER

Раздел HKEY_LOCAL_MACHINE

Информация о выбранной политике безопасности хранится в следующих ветках реестра Windows XP:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies

Вход в Windows

Автоматический вход в Windows

Регистрационные данные

Диспетчер задач Windows

Пароль после ждущего режима

Автозагрузка

Форма отчетности:

1. Титульный лист
2. Содержание
3. Задание
4. Описание выполнения каждого пункта задания
5. Выводы

Задания для самостоятельной работы:

Проанализировать специфику работы с реестром.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Работа с реестром в Windows

Реестр - база данных операционной системы, содержащая конфигурационные сведения. Физически вся информация реестра разбита на несколько файлов. Реестры Windows 9x и NT частично различаются. В Windows 95/98 реестр содержится в двух файлах SYSTEM.DAT и USER.DAT, находящиеся в каталоге Windows. В Windows Me был добавлен еще один файл CLASSES.DAT. В Windows XP реестр хранится во многих файлах. Основная часть хранится в файлах sam, security, software, system, default (все файлы без расширения). По замыслу Microsoft он должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы. Почему произошел переход от ini файлов к реестру? Дело в том, что на эти файлы накладывается ряд серьезных ограничений, и главное из них состоит в том, что предельный размер такого файла составляет 64Кб. ПРЕДУПРЕЖДЕНИЕ: НИКОГДА не удаляйте или не меняйте информацию в реестре, если Вы не уверены что это именно то, что нужно. В противном случае некорректное изменение данных может привести к сбоям в работе Windows и, в лучшем случае, информацию придется восстанавливать из резервной копии. Раздел HKEY_CURRENT_USER является подразделом раздела HKEY_USERS (HKEY_USERS содержит все активные загруженные профили пользователей компьютера). HKEY_CURRENT_USER является корневым для данных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, параметры рабочего стола, сетевых подключений, принтеров и приложений. Эти сведения сопоставлены с

профилем пользователя. Вместо полного имени раздела иногда используется аббревиатура HKCU.

Параметры текущего пользователя делятся на несколько категорий: AppEvents - содержит пути звуковых файлов, используемых для озвучивания системных событий.

Control Panel - содержит различные данные, которые могут быть изменены в панели управления.

Display - содержит пользовательские установки экрана для текущего пользователя (этот подраздел доступен, только если разрешены пользовательские профили (user profiles)). InstallLocationsMRU - содержит пути, использованные в процессе последней инсталляции. Keyboard layout - содержит информацию о раскладке клавиатуры. Текущая раскладка клавиатуры устанавливается с использованием пункта Клавиатура (Keyboard) панели управления.

Network - содержит подразделы, описывающие постоянные и недавно установленные сетевые соединения, а также состояние сети.

RemoteAccess - необязательный подраздел, доступный только в случае, если установлен сервис удалённого доступа.

SOFTWARE- содержит пользовательские настройки приложений. Этот раздел ссылается на раздел HKEY_LOCAL_MACHINE, в которой также хранятся настройки приложений. Раздел HKEY_LOCAL_MACHINE определяет всю информацию, относящуюся к локальному компьютеру, такую как драйверы, установленное программное обеспечение, наименование портов и конфигураций программного обеспечения. Эта информация верна для всех пользователей, подключённых к системе.

Раздел HKEY_LOCAL_MACHINE состоит из нескольких подразделов: Hardware - хранит информацию об устройствах, обнаруженных в компьютере. Все параметры этого раздела хранятся не на жестком диске, а в оперативной памяти. Когда компьютер распознает запуск устройства, он нумерует найденное устройство, исследуя шину и отдельные классы устройств (например, порты или клавиатуру).

Security - Здесь содержится всевозможная информация, относящаяся к защите. Формат не документирован. Используется для кэширования верительных данных для входа в систему, настроек политики и разделяемых секретных данных сервера. Подраздел Security\SAM содержит копию большинства данных из HKLM\SAM.

Sam - Здесь хранятся локальные учетные записи или группы, созданные на компьютере. Раздел скрыт.

Software - вся информация о программах, установленных на компьютере, хранится здесь.

System\CurrentControlSet - Последним действием фазы загрузки Windows является обновление реестра, которое должно зафиксировать набор служб и управляющих настроек, применявшийся при последней успешной загрузке. CurrentControlSet всегда указывает на набор управляющих настроек, используемых системой в текущий момент System\MountedDevices - Тома динамических дисков зависят от наличия информации о текущей конфигурации о логических томах на диске. Приложения и оснастки берут эту информацию из службы Logical Volume Manager, которая хранит свой список смонтированных и доступных устройств и подразделе MountedDevices.

Информация о выбранной политике безопасности хранится в следующих ветках реестра Windows XP:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies

Вход в Windows

Автоматический вход в Windows

Существует возможность автоматического входа в Windows, минуя экран приветствия. Данный способ не совсем безопасен, так как любой может войти в систему, если не требуется вводить пароль. Для автоматического входа в систему требуется изменить строковый параметр AutoAdminLogon на 1 в разделе

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

Также необходимо установить строковые значения DefaultUserName и DefaultPassword в этом же разделе равными имени пользователя и пароля, которые используются для входа в Windows. Возможно, вам также придется установить строковое значение DefaultDomainName, если ваш компьютер используется как домен. Однако, вы должны понимать, что при автоматическом входе любой пользователь, получивший доступ к вашему компьютеру, может узнать ваш пароль, который хранится в реестре в открытом виде.

Лимит на число попыток автоматического входа в Windows

Данная настройка является логическим продолжением предыдущей настройки. Можно задать число попыток для автоматического входа в Windows. В этом случае в том же разделе надо создать параметр Dword AutoLogonCount и присвоить ему некоторое значение. Например, если вы присвоите значение 5, то система пять раз автоматически войдет в Windows. Причем, при каждом входе данный параметр в реестре будет автоматически уменьшаться на единицу. Когда значение параметра достигнет 0, ключи AutoLogonCount и DefaultPassword будут удалены из реестра, а параметру AutoAdminLogo будет присвоено значение 0.

Регистрационные данные

Если вы нажмете на пункт меню О программе в Проводнике или в других программах, поставляемых с Windows, то увидите, кто обладает правом использования этой копии. Также эти данные можно увидеть в апплете Система Панели управления. Возможно, вам компьютер достался от вашего босса Пупкина, и вы хотели бы изменить регистрационные данные. Для этого нужно изменить строковые параметры RegisteredOwner (Ваше имя) и RegisteredOrganization (название организации) в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion

Диспетчер задач Windows

Чтобы запретить пользователю возможность запуска Диспетчера задач Windows, установите значение параметра типа DWORD DisableTaskMgr в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System равным 1

Пароль после ждущего режима

Можно настроить систему таким образом, чтобы при включении компьютера после Ждущего режима появлялось диалоговое окно с приглашением ввести пароль. Для этого в разделе

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Power создаем параметр типа DWORD PromptPasswordOnResume со значением 1.

Автозагрузка

Что скрывается в автозагрузке?

Существует несколько способов прописать программу в автозагрузку. Самый простой - скопировать программу или ярлык в папку Автозагрузка. Но существует другой способ - через реестр. Этим способом часто пользуются вредоносные программы (вирусы, трояны, шпионы)

Сперва откройте раздел

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion.

Найдите там подразделы Run, RunOnce В этих разделах есть строковые ключи (некоторые разделы пустые), отвечающие за запуск программ. Название ключа может быть произвольным, а в качестве значения у них указывается запускаемая программа, если надо - то с параметрами. Обратите внимание на разделы, в названии которых присутствует "Once". Это разделы, в которых прописываются программы, запуск которых надо произвести всего один раз. Например, при установке новых программ некоторые из них прописывают туда ключи, указывающие на какие-нибудь настроечные модули, которые запускаются сразу после перезагрузки компьютера. Такие ключи после своего запуска автоматически удаляются. Проверьте, что за программы у вас запускаются. Все ли они нужны вам при загрузке и лишнее удалите. Это позволит значительно ускорить загрузку Windows.

В разделе

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion есть только два подраздела, отвечающие за автозагрузку: Run и Runonce. Изначально они пустые, так что все записи сделаны другими программами

Запрет на автозагрузку

Существуют способы наложения запрета на автозагрузку программ через записи в реестре, указанные выше. Используются параметры типа DWORD. Все параметры должны храниться в разделе

HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Policies\Explorer

Для запрета запуска программ, прописанных в подразделе Run раздела LOCAL MACHINE используется параметр DisableLocalMachineRun со значением 1. В этом случае система игнорирует содержимое списка Run, находящегося в LOCAL MACHINE. Аналогично действует запрет списка Run Once для LOCAL MACHINE. За состояние этой политики отвечает параметр DisableLocalMachineRunOnce. Система игнорирует содержимое RunOnce в LOCAL MACHINE.

Для запрета списка Run раздела CURRENT USER используется параметр DisableCurrentUserRun.

Для запрета списка Run Once раздела CURRENT USER используется параметр DisableCurrentUserRunOnce

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

4. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
5. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?
2. Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?
3. Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?
4. Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?

Лабораторная работа №2 Анализ угроз информационной безопасности.

Цель работы: Ознакомиться с алгоритмами анализа угроз информационной безопасности.

Задание:

Произвести оценку ценности информационного актива на основании возможных потерь для организации в случае реализации угрозы согласно индивидуальному варианту.

Порядок выполнения:

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D**и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).

4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ
8. Оценка рисков
9. Выводы

Задания для самостоятельной работы: Вариант задания соответствует порядковому номеру в списке студентов группы.

1. Поликлиника
2. Колледж
3. Офис страховой компании
4. Рекрутинговое агентство
5. Интернет-магазин
6. Центр оказания государственных услуг
7. Отделение полиции
8. Аудиторская компания
9. Дизайнерская фирма
10. Офис интернет-провайдера

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Риск ИБ – потенциальная возможность использования определенной **угрозойуязвимостейактива** или группы активов для причинения вреда организации.

Уязвимость- слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Что такое Риск ИБ.
2. Понятие уязвимости.
3. Виды угроз ИБ.
4. Охарактеризуйте информационные активы, приведите примеры.

Лабораторная работа №3 Реализация систем парольной защиты и их анализ.

Цель работы: Изучение технологии аутентификации пользователя на основе пароля.

Задание:

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля.

Порядок выполнения:

1. В качестве информационного ресурса использовать любой файл или приложение.
2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям.
3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.
4. Пользователь должен иметь возможность поменять пароль

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Текст программы
5. Пример работы программы
6. Уязвимости системы защиты информации
7. Выводы

Задания для самостоятельной работы: Вариант задания соответствует порядковому номеру в списке студентов группы.

1. Поликлиника
2. Колледж
3. Офис страховой компании
4. Рекрутинговое агентство
5. Интернет-магазин
6. Центр оказания государственных услуг
7. Отделение полиции
8. Аудиторская компания
9. Дизайнерская фирма
10. Офис интернет-провайдера

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авто-

ризованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Риск ИБ – потенциальная возможность использования определенной Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.

Для справки: Пример поиска элемента в массиве (Delphi):

```
// ввод массива for i:=l to SIZE do
a[i] := StrToInt(StringGridl.Cells[i - 1, 0]);
// ввод образца для поиска
obr := StrToInt(edit2.text);
// поиск
found := FALSE; // пусть нужного элемента в массиве нет
i := 1;
repeat
if a[i] = obr then
found := TRUE
else
i := i + 1;
until (i > SIZE) or (found = TRUE);
```

3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.

4. Пользователь должен иметь возможность поменять пароль

Используемые символы	Дополнительные средства защиты
Латиница (строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.
Кириллица (строчные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
Цифры	Применение метода аутентификации на основе одноразовых паролей: каждый следующий пароль=предыдущий пароль+5
Цифры+ знаки арифметических операций	При смене пароля: проверка на отсутствие повторяющихся символов.
Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (храниться в системе) в формате дд.мм.гг или дд/мм/гг
Латиница (прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: при каждой следующей попытке входа в систему последняя буква пароля меняется на следующую по алфавиту.
Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с фамилией пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (храниться в системе) в формате дд.мм.гггг или дд/мм/гггг

Цифры	Применение метода аутентификации на основе одноразовых паролей: к первой цифре каждого следующего пароля прибавляется 1.
Кириллица (прописные и строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.
Латиница (строчные и прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля к нему добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение.(в качестве «случайной» величины использовать «Abc»)
Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с отчеством пользователя.
Цифры	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxxxxxxxxx.
Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий месяцев).
Латиница (строчные и прописные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Что такое парольная защита.
2. Как осуществляется алгоритм аутентификации пользователя.

Лабораторная работа №4 Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра.

Цель работы: получение практических навыков защиты программного обеспечения от несанкционированного доступа.

Задание:

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра.
2. Включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE).
3. Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра (если лабораторная работа выполняется в операционной системе Windows).
4. Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

Порядок выполнения:

Вход в Windows

Автоматический вход в Windows
Регистрационные данные
Пароль после ждущего режима
Автозагрузка
Автозапуск CD-ROM
Запрещение запуска программ
Запрещение запуска редактора реестра
Пароли и безопасность
Отмена кэширования пароля
Звездочки в паролях
Запрет перечисления рабочей группы
Раскладка клавиатуры
Раскладка для окна Приветствие
Клавиша Windows
Отключение клавиши Windows
Запрещение горячих клавиш с клавишей Windows
Длинные и короткие имена файлов
Запрещение длинных имен файлов
Запрет сохранения паролей в Dial-Up-соединениях

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Описание выполнения каждого пункта задания
5. Выводы

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Вход в Windows

Автоматический вход в Windows

Существует возможность автоматического входа в Windows, минуя экран приветствия. Данный способ не совсем безопасен, так как любой может войти в систему, если не требуется вводить пароль. Для автоматического входа в систему требуется изменить строковый параметр AutoAdminLogon на 1 в разделе

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

Также необходимо установить строковые значения DefaultUserName и DefaultPassword в этом же разделе равными имени пользователя и пароля, которые используются для входа в Windows. Возможно, вам также придется установить строковое значение DefaultDomainName, если ваш компьютер используется как домен. Однако, вы должны понимать, что при автоматическом входе любой пользователь, получивший доступ к вашем компьютеру, может узнать ваш пароль, который хранится в реестре в открытом виде.
Лимит на число попыток автоматического входа в Windows
Данная настройка является логическим продолжением предыдущей настройки. Можно задать число попыток для автоматического входа в Windows. В этом случае в том же разделе надо создать параметр Dword AutoLogonCount и присвоить ему некоторое значение. Например, если вы присвоите значение 5, то система пять раз автоматически войдет в Windows. Причем, при каждом входе данный параметр в реестре будет автоматически уменьшаться на единицу. Когда значение параметра достигнет 0, ключи **AutoLogonCount** и **DefaultPassword** будут удалены из реестра, а параметру **AutoAdminLogo** будет присвоено значение 0.

Регистрационные данные

Если вы нажмете на пункт меню О программе в Проводнике или в других программах, поставляемых с Windows, то увидите, кто обладает правом использования этой копии. Также эти данные можно увидеть в апплете Система Панели управления. Возможно, вам компьютер достался от вашего босса Пупкина, и вы хотели бы изменить регистрационные данные. Для этого нужно изменить строковые параметры RegisteredOwner (Ваше имя) и

RegisteredOrganization (название организации) в разделе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion

Диспетчер задач Windows

Чтобы запретить пользователю возможность запуска **Диспетчера задач Windows**, установите значение параметра типа **DWORD** DisableTaskMgr в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System равным 1

Пароль после ждущего режима

Можно настроить систему таким образом, чтобы при включении компьютера после **Ждущего режима** появлялось диалоговое окно с приглашением ввести пароль. Для этого в разделе

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Power создаем параметр типа DWORD PromptPasswordOnResume со значением 1.

Автозагрузка

Что скрывается в автозагрузке?

Существует несколько способов прописать программу в автозагрузку. Самый простой - скопировать программу или ярлык в папку Автозагрузка. Но существует другой способ - через реестр. Этим способом часто пользуются вредоносные программы (вирусы, трояны, шпионы)

Сперва откройте раздел

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion.

Найдите там подразделы Run, RunOnce В этих разделах есть строковые ключи (некоторые разделы пустые), отвечающие за запуск программ. Название ключа может быть произвольным, а в качестве значения у них указывается запускаемая программа, если надо - то с параметрами. Обратите внимание на разделы, в названии которых присутствует "Once". Это разделы, в которых прописываются программы, запуск которых надо произвести всего один раз. Например, при установке новых программ некоторые из них прописывают туда ключи, указывающие на какие-нибудь настроечные модули, которые запускаются сразу после перезагрузки компьютера. Такие ключи после своего запуска автоматически удаляются. Проверьте, что за программы у вас запускаются. Все ли они нужны вам при загрузке и лишнее удалите. Это позволит значительно ускорить загрузку Windows.

В разделе

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion

есть только два подраздела, отвечающие за автозагрузку: Run и Runonce. Изначально они пустые, так что все записи сделаны другими программами

Запрет на автозагрузку

Существуют способы наложения запрета на автозагрузку программ через записи в реестре, указанные выше. Используются параметры типа **DWORD**. Все параметры должны храниться в разделе

HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Policies\Explore

Для запрета запуска программ, прописанных в подразделе Run раздела LOCAL MACHINE используется параметр DisableLocalMachineRun со значением 1. В этом случае система игнорирует содержимое списка **Run**, находящегося в **LOCAL MACHINE**. Аналогично действует запрет списка Run Once для LOCAL MACHINE. За состояние этой политики отвечает параметр DisableLocalMachineRunOnce. Система игнорирует содержимое **RunOnce в LOCAL MACHINE.**

Для запрета списка **Run** раздела **CURRENT USER** используется параметр DisableCurrentUserRun.

Для запрета списка **Run Once** раздела **CURRENT USER** используется параметр DisableCurrentUserRunOnce

Автозапуск CD-ROM

Отключение стандартного автозапуска компакт-дисков

Чтобы отключить автозапуск компакт-диска, устанавливаем значение параметра типа **DWORD** AutoRun, равным 0 в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom

Запрещение запуска программ

Windows позволяет ограничить доступ к программам, кроме разрешенных в специальном списке.

Для ограничения запускаемых программ надо открыть раздел HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVerson\Policies\Explorer и создать там ключ RestrictRun типа DWORD со значением 0x00000001. Затем тут же надо создать подраздел с аналогичным именем RestrictRun и в нем перечислить список РАЗРЕШЕННЫХ к запуску программ для текущего пользователя. Записи в этом подразделе пронумеровываются, начиная с 1, и содержат строки с путями (необязательно) и именами приложений. Файлы должны быть с расширением. Например, Word.exe, Excel.exe ... Не забудьте указать файл Regedit.exe, иначе Вы сами не сможете больше запустить редактор реестра! Для сброса ограничения на запуск программ надо установить значение ключа RestrictRun в 0

Запрещение запуска редактора реестра

Вы можете запретить запуск редактор реестра

Для этого в разделе

HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\CurrentVerson\Policies\System нужно добавить ключ типа DWORD DisableRegistryTools со значением 1. Запуск редактора реестра будет запрещен, однако останется возможность вносить изменения с помощью программного обеспечения сторонних разработчиков и с помощью REG-файла

Пароли и безопасность

Рассматриваемые настройки хранятся в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network Все ключи имеют тип **DWORD**, если это не обговорено отдельно; значение ключа равное 1 включает данную опцию, 0 выключает, если это не обговорено отдельно

Отмена кэширования пароля

Данная настройка помогает избавиться от проблемы "утаскивания" и дальнейшего взлома ваших сетевых и интернет паролей. Эти пароли хранятся в файле с расширением PWL. Отключение кэша запрещает запись паролей в этот файл. Следовательно, его "выкрадывание" и дальнейший взлом не приносят никаких результатов. Единственное неудобство - это надобность вводить каждый раз при коннекте в окно DialUp - Password пароль вручную. Но это всё же лучше, чем "подарить" пароль и логин хакеру. Итак, используем параметр типа DisablePwdCaching со значением 1 Находим в каталоге Windows файл (или файлы) с расширением PWL. Удаляем их. Перезагружаемся. Файл паролей хоть и создаётся опять, но он пустой

Звездочки в паролях

Параметр типа HideSharePwds со значением 1 определяет, показывать ли пароли к расшаренным ресурсам (имеющим общий доступ) открытым текстом или заменять их звездочками.

Запрет перечисления рабочей группы

Для того чтобы запретить перечисление содержимого рабочей группы, надо установить значение ключа NoWorkgroupContents равным 1.

Даже при запрете пользователи могут подключаться к компьютерам в своей рабочей группе или домене. Для этого необходимо набрать полное сетевое имя разделенного ресурса в формате UNC, в диалоговых окнах команд "Выполнить" или "Подключить сетевой диск".

Раскладка клавиатуры

Раскладка для окна Приветствие

Если при установки системы вы в качестве основного языка установили русский язык, а пароль обычно используете на английском языке, то при выводе окна **Приветствие** вам каждый раз придется переключаться с русского языка на английский, чтобы ввести пароль.

Чтобы по умолчанию система выводила английскую раскладку в этом окне надо открыть раздел

HKEY_USERS\.DEFAULT\Keyboard Layout\Preload

И там надо на первую позицию поместить желаемую раскладку - 00000409 (английская раскладка) или 00000419 (русская), т.е. просто поменяйте их местами.

Клавиша Windows

Отключение клавиши Windows

На некоторых современных клавиатурах присутствует клавиша Windows (как правило, логотип-флажок Майкрософт). Некоторым пользователям она мешает при быстрой печати или играх. Чтобы отключить ее, нужно создать новый двоичный параметр Scancode Map со значением **00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00** в разделе

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout

Запрещение горячих клавиш с клавишей Windows

Можно отключить использование комбинацию "горячих" клавиш с клавишей Windows. Для этого создаем параметр типа **DWORD** NoWinKeys со значением 1 в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer Однако после установки этого запрета, одиночное нажатие клавиши Windows, которое вызывает меню "Пуск", будет работать.

Длинные и короткие имена файлов

Запрещение длинных имен файлов

Вы можете запретить длинные имена файлов в Windows, заставив тем самым генерировать имена в формате 8.3 (DOS-овский формат). Для этого в разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem надо изменить параметр Win31FileSystem, присвоив ему значение 01 (по умолчанию стоит 00) Сделанные изменения вступят в силу после перезагрузки

Установка способа доступа к расшаренным ресурсам компьютера из сети (Windows NT/2000/XP)

Раздел: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Параметр типа DWORD RestrictAnonymous

Если значение равно 1 - запрещает анонимным юзерам просматривать удаленно учетные записи и расшаренные ресурсы. 2 - отказывает любой неявный доступ к системе (в сетевом окружении компьютер не будет виден, однако, доступ к нему можно будет получить, обратившись к нему по его IP).

Запрет сохранения паролей в Dial-Up-соединениях

По умолчанию, в Dial-Up-соединениях введенный пароль сохраняется после успешного соединения, если задействована опция "Сохранять имя пользователя и пароль", расположенная на диалоговом окне для Dial-Up. Это достаточно удобно для многих пользователей, но если вы занимаетесь проблемой безопасности системы, то можете запретить сохранение этих паролей. В разделе

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

создайте параметр типа **DWORD** DisableSavePassword со значением 1, который запрещает сохранение паролей в Dial-Up-соединениях. В этом случае опция "Сохранять имя пользователя и пароль" становится недоступной, а сохраненные пароли пропадают.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/

А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Принципы классификации систем защиты программного обеспечения (ПО).
2. Классификация систем защиты ПО по методу установки.
3. Классификация систем защиты ПО по используемым механизмам защиты.
4. Классификация систем защиты ПО по принципу функционирования.
5. Назначение упаковщиков-шифраторов.
6. Системы защиты от несанкционированного копирования.

Лабораторная работа №5 Исследование нормативно-правовой базы информационной безопасности предприятия.

Цель работы: проанализировать документы и акты, составляющие нормативно-правовую базу информационной безопасности предприятия.

Задание:

а) Описать структуру предприятия, с указанием отделов и их функциями, приложить схему структуры предприятия

б) Проанализировать и описать угрозы для предприятия, к каждой угрозе подписать тот отдел, который наиболее уязвим от этой угрозы.

в) Проанализировать и описать модели злоумышленников.

с) Требования гарантии безопасности оформить в виде таблицы по отделам

д) Разработать должностную инструкцию сотруднику, ответственному за защиту информации.

е) Разработать Инструкцию о порядке ввода в эксплуатацию объектов электронной вычислительной техники, допуска сотрудников к работе на ПЭВМ, и соблюдению требований собственной безопасности при обработке закрытой информации на собственной вычислительной технике.

Порядок выполнения:

Изучить модель угроз ИБ на заданном предприятии

Описать структуру предприятия.

Проанализировать и описать угрозы для предприятияэ

Проанализировать и описать модели злоумышленников.

Провести сравнительный анализ отдельных вопросов защиты информации в зарубежных и отечественных документах

Разработать документы по обеспечению информационной безопасности на предприятии

Сформулировать выводы по результатам исследований

5. Пользователь должен иметь возможность поменять пароль

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Описание выполнения по шагам
5. Выводы

Задания для самостоятельной работы: Вариант задания по выбору предприятия соответствует порядковому номеру в списке студентов группы.

1. Поликлиника
2. Колледж
3. Офис страховой компании
4. Рекрутинговое агентство
5. Интернет-магазин
6. Центр оказания государственных услуг
7. Отделение полиции
8. Аудиторская компания
9. Дизайнерская фирма
10. Офис интернет-провайдера

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Информационная безопасность – это весьма важный вопрос для любой компании. В серьезных компаниях вопросами защиты информации и безопасности данных занимаются специально обученные люди — сисадмины (системные администраторы) или обишники (инженеры по обеспечению безопасности информации). От большинства простых пользователей они отличаются тем, что, даже разбуженные ночью или в пьяном угаре, как отче наш проговорят три принципа защиты информации на компьютере.

Принцип предотвращения подразумевает, что лучше избежать проблемы, чем заполучить ее, героически с ней сражаться и с блеском решить.

Принцип обнаружения сводится к тому, что, если предотвратить неприятность не удалось, своевременное ее обнаружение в большинстве случаев способно свести неприятности к минимуму. Если вы ненароком подцепили вирус (компьютерный, хотя для болезнетворных вирусов принцип также работает), то быстро начатое лечение способно пресечь разрушительные действия паразита.

Принцип восстановления гласит, что данные, которые могут быть утеряны, обязательно должны храниться в виде резервных копий. Что подойдет лично вам — дискетки, магнитооптика, CD-RW или “брелки” с flash-карточкой, — вам же и решать. Вариантов современная компьютерная индустрия предлагает множество. Даже методы форматирования жестких дисков развиваются согласно принципам восстановления и защиты информации.

Прошли те времена, когда хакерами были специалисты, детально знающие компьютерную технику и способные творить чудеса с программным кодом. Сейчас любой усидчивый, любознательный, но особо не обремененный моральными принципами подросток способен создать рядовому пользователю массу проблем. За примерами далеко ходить не надо, достаточно почитать “Новости интернета”. По нескольку раз в месяц разгораются скандалы или целые судебные разбирательства, связанные с молодыми людьми, запустившими новый почтовый червь, взломавшими сервер банка, компьютеры министерства обороны США... Как правило, такие хулиганы попадаются из-за собственной невнимательности или желания прославиться. При соблюдении мер предосторожности мошенников в сфере высоких технологий вычислить весьма трудно. В частности, именно поэтому преступлениями в сфере информационных технологий занимается Интерпол.

Злоумышленнику, для того чтобы получить доступ к конфиденциальной информации, порой не требуется даже специальных навыков и умений. Во многих случаях срабатывает человеческий фактор, например бумажка с написанным паролем на мониторе или под стеклом возле клавиатуры. Пароли, как правило, тоже оригинальностью не отличаются. А в недрах интернета всегда можно найти программы, которые возьмут на себя рутинную работу по перебору наиболее очевидных паролей.

Сейчас любой, даже слабо разбирающийся в компьютерах, хулиган за 15 минут найдет в интернете с десяток программ для подбора пароля из 4—6 символов и предоставляющих доступ к удаленному компьютеру. А ведь помимо хакеров есть еще и фрикеры, специализирующиеся на взломе электронных устройств, в частности, на сотовых телефонах, и кардеры, взламывающие пароли и подбирающие номера к кредиткам.

Из этого следует, что к вопросу информационной безопасности следует подходить серьезно и с полной отдачей.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Перечислите основные документы по информационной безопасности предприятия.
2. Какие локальные нормативные акты могут существовать на предприятии, для обеспечения ИБ.

Лабораторная работа №6 Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.

Цель работы: Изучение алгоритмов вызова программ в ОС MS DOS, а также принципов действия атак переполнения буфера ("buffer-overflow"). Применение ос нов информационной безопасности для нахождения путей противодействия угрозе. Реализация на практике модели атаки переполнения буфера в ОС MS DOS.

Задание:

Написать четыре программы:

- программу, подверженную атаке переполнения буфера;
- программу, защищенную от атак данного типа;
- программу, реализующую атаку переполнения буфера; -
программу типа EXPLOIT.

Проанализировать проделанную работу и предложить свой метод использования модификации адреса возврата.

Порядок выполнения:

Изучить алгоритмы вызова программ в ОС MS DOS

Изучить принципы действия атак переполнения буфера ("buffer-overflow").

Реализовать алгоритмы на практике модели атаки переполнения буфера в ОС MS DOS.

Сформулировать выводы по результатам исследований

6. Пользователь должен иметь возможность поменять пароль

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Описание выполнения по шагам
5. Выводы

Задания для самостоятельной работы: предложить свой метод использования модификации адреса возврата.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Известно, что в результате некорректного обращения к памяти может возникнуть проблема с менеджером памяти или зависание.

Как правило, это связано с тем, что программа попыталась получить доступ к не принадлежа- щей ей области памяти. Это довольно часто случается, если программист за- был, например, проверить размеры строки, заносимой в буфер, и остаток строки попал в какие-то другие данные или даже в код. Это происходит из-за отсутствия контроля за размерами строк и буферов. Логичным следствием является наличие так называемых "buffer-overflow"-программ, которые в защищенных операционных системах используются для нарушения защиты системы и получения привилегий суперпользователя системы (в данной лабораторной работе в качестве модели используется ОС MS DOS).

Рассмотрим две программы, которые подвергаются атакам "bufferoverflow". Их отличие состоит в том, что одна из них подвержена атаке, а другая – нет. Обе программы имеют статически определенный буфер конечного размера и принимают в качестве параметра строку неизвестной длины, которая заносится в этот буфер, признаком конца строки является нулевой символ.

Во второй программе присутствует проверка на допустимую длину строки, в первой нет. Для демонстрации работы этих двух программ необходимо написать специальную "buffer-overflow"-программу, которая вызывает программу-цель в режиме «с возвратом в предок» с параметром-строкой произвольного раз- мера. Рассмотрим изменение состояния стека в процессе вызова программы цели.

Компилятор, встречая инструкцию вызова функции main(), заносит в стек смещение следующей после вызова команды.

Таким образом, функция main() завершив свою работу, будет знать адрес возврата управления. В результате стек (область младших адресов) ← Указатель вершины стека RETADR ← Адрес возврата PARAMS ← Параметры функции Использованная часть стека (область старших адресов

Функции надо запомнить указатель на текущую верхушку стека BP, который будет использоваться в ссылке на параметры. Поэтому, независимо от архитектуры, выполняются следующие две инструкции, push bp mov bp, sp Теперь в верхушке стека лежит предыдущее значение регистра BP, а сам он указывает на верхушку стека и может быть использован в качестве ба- зового регистра при ссылке на параметры.

В программах объявлен размер буфера в SIZE байт – этот буфер будет зарезервирован в стеке.

После всего этого программа работает прекрасно, пока дело не доходит до вызова функции strcpy(). Если длина строки меньше или равна длине буфера, то все пройдет хорошо, функция отработает, освободит зарезервированное пространство, восстановит регистр BP и вернет управление программе, которая очистит стек от переданных параметров.

Если же длина строки будет больше размера буфера, то поскольку strcpy() копирует все символы, пока не встретит код конца строки – 0, часть строки затрет верхнюю часть стека и может испортить поле RETADR. Это станет заметно не сразу – все будет работать корректно, пока дело не дойдет до вызова return.

Управление будет передано по адресу, который хранится в поле RETADR, но поскольку адрес испорчен, программа будет продолжать выполняться в некоторой точке адресного пространства, отличающейся от точки вызова. В этом месте воз- 22 никнет исключительная ситуация, и программа будет аварийно прервана, поскольку маловероятно, чтобы адрес возврата указывал на какой-то осмысленный код, причем находящийся в области памяти данной программы. (область младших адресов) ← Указатель вершины стека ????? ← Начало зарезервированного буфера ????? ????? ← Конец буфера OLDBP ← Старое значение регистра BP RETADR ← Адрес возврата PARAMS ← Параметры функции

Избежать подобной ситуации можно по крайней мере двумя способами.

Первый способ - контроль длины строки, копируемой в буфер. Этот способ необходимо реализовать в программе под номером

Второй способ несколько необычен, но именно он помогает понять действие "buffer-overflow"-программ.

Назовем программу, реализующую этот метод OVERFLOW. он состоит в следующем: - файл-цель исследуется с помощью отладчика, например “Turbo Debugger”. Необходимо узнать BP и RETADR; - программа OVERFLOW.EXE вызывает программу-цель с параметром – строкой, которая «затирает» поля BP и RETADR старыми, заранее известными значениями этих полей. Параметром программы OVERFLOW.EXE является имя файла, содержащего имя программы-цели (это поле должно зани- мать 13 символов), BP и RETADR (значения должны быть записаны в HEX - формате). На практике для исследования программы-цели применяются так называемые EXPLOIT-программы.

Их целью является осуществление атаки для формальной проверки исследуемой программы на устойчивость. EXPLOITпрограмма запускает программу-цель со строкой переменной длины до тех пор, пока программа – цель не зависнет или не сообщит об ошибке. Если программа зависла, это означает, что в ней отсутствует проверка на длину входной строки.

Следовательно, данная программа не защищена от атаки переполнения буфера. Программа должна запускаться с двумя параметрами: - имя программы-цели; - предельная длина строки. В результате работы программы на экран дисплея должно выводится сообщение о текущем размере строки, передаваемой в качестве параметра программе-цели. Если весь вывод перенаправить в файл, то в случае успешной атаки, то есть зависания системы, в этом файле можно будет узнать размер последней строки. Таким образом, можно узнать размер буфера программы-цели.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Каковы основные направления обеспечения информационной безопасности объектов информационной сферы государства?
2. Дайте классификацию методов нарушения конфиденциальности, целостности и доступности информации.
3. В чем заключается атака переполнения буфера?
4. Каковы могут быть последствия атаки в различных операционных системах?
5. Какие алгоритмы противодействия атаке переполнения буфера Вам известны?
6. Какие ошибки в программном обеспечении используются EXPLOITпрограммами?

Лабораторная работа №7 Причины, виды, каналы утечки и искажения информации.

Цель работы: Изучение основных задач, моделирование и реализация на практике процесса регистрации и учета событий в ОС MS-DOS с целью практического применения основ защиты информации, а также для ознакомления с системой прерываний данной операционной системы.

Задание:

Написать на языке Си программу, реализующую протоколирование всех нажатий клавиш в файле аудита клавиатуры, а также времени их нажатия. Исключение составляют триггерные клавиши, для них необходимо фиксировать только те нажатия, которые влияют на смену их состояния.

Порядок выполнения:

Написать на языке Си программу, реализующую протоколирование всех нажатий клавиш в файле аудита клавиатуры, а также времени их нажатия.

Программа должна позволять выполнять любые операции операционной системы и не должна мешать работе других программ, то есть она должна работать в так называемом фоновом режиме.

Файл аудита клавиатуры должен иметь имя, длиной не более восьми символов, которое должно быть уникальными для каждого пользователя.

Необходимо реализовать предотвращение повторного запуска программы-аудита и отгрузку ее из памяти, то есть управление резидентной частью.

Пользователь, выполняющий роль администратора аудита, должен иметь следующие возможности в части запуска и отключения аудита: - временное отключение аудита; - определение информации о состоянии аудита (установлен или нет); - задание идентификационного имени пользователя, для которого необходимо запускать аудит (не должно превышать восьми символов); - располагать файлы аудита удобным для администратора образом, т.е. файл аудита не должен быть жестко привязан ни к какому конкретному каталогу или диску.

Сформулировать выводы по результатам исследований

7. Пользователь должен иметь возможность поменять пароль

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Алгоритм функционирования программы в фоновом режиме.
5. Алгоритм предотвращения повторного запуска, отгрузки программы.
6. Алгоритм обхода нереентерабельности в ОС MS-DOS.
7. Выводы

Задания для самостоятельной работы: Проанализировать проделанную работу с целью нахождения путей применения аудита клавиатуры. В качестве альтернативы можно придумать и реализовать свою программу обработки результатов аудита клавиатуры.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Так как MS-DOS является однозадачной операционной системой, то в определенный момент времени в ней может работать только один пользователь, поэтому в программе аудита должен присутствовать механизм идентификации, позволяющий для каждого пользователя определить идентификационное имя, которое используется для наименования файла аудита.

Файл аудита содержит информацию о действиях пользователя в системе: - время входа с систему (время запуска программы-аудита); - специальная информация, которая зависит от назначения аудита. Специальная информация определяется целью аудита.

Цель аудита – фиксирование попыток со стороны пользователя осуществить неавторизованные, то есть недозволенные, действия, а также те действия, которые могут повлечь за собой нарушение работоспособности системы

Примеры неавторизованных действий: - работа за терминалом в недозволенное время. Определяется с помощью аудита клавиатуры путем анализа времени протоколирования нажатия на клавишу; - запуск программ. приводящий к нарушению работоспособности операционной системы.

Определяется с помощью аудита клавиатуры, если команда на запуск программы поступает из командной строки, а не с помощью другой программы. Административные ограничения могут накладываться также на функции создания, удаления, переименование файлов и каталогов. Такие контролирующие действия вынуждают пользователя быть дисциплинированным. Таким образом, аудит – средство, позволяющее проверять выполнение требований, предъявляемых пользователю администратором системы, отвечающим за нормальное функционирование операционной системы и целостность хранящихся в ней данных.

Выполнение программы в фоновом режиме возможно, благодаря возможности создания резидентных программ. Отличительное свойство резидентных программ (TSR – Terminate-but-Stay-Resident) СОСТОИТ В ТОМ, ЧТО ОНИ после своего завершения остаются в памяти компьютера, а операционная система помечает занятую ими память как используемую.

Использование TSR позволяет реализовать так называемое пассивное мультипрограммирование MS-DOS является однопрограммной операционной системой, но активизация TSR вызывает переключение компьютера на резидентную программу. Если активизация TSR выполняется периодически, появляется возможность выполнения программ на фоне других программ. Следующее обязательное требование к надежно работающей TSR – предотвращение повторного вхождения в MS-DOS.

Однопрограммная MSDOS не является реентерабельной. Реентерабельная программа – это про- грамма, которая разрешает в силу особенностей своего построения, начинать ее выполнение несколько раз, не дожидаясь завершения выполнения (выхода) программы, начатого ранее. Реентерабельная программа не изменяет ни одной константы или переменной, которые могут повлиять на повторное выполнение программы. Большинство программ, образующих в совокупности ядро MS-DOS, не являются реентерабельными. В этой связи не являются реентерабельными и программы, обращающиеся к функциям MS-DOS непосредственно, либо через функции библиотеки языка Си.

Для TSR, написанной на языке Си, всегда существует вероятность повторного

вхождения в MS-DOS, так как TSR может получить управление в любой момент, в том числе и тогда, когда MS-DOS выполняет нереентерабельную секцию своего кода.

Отсюда следует требование к ISR активизировать TSR только тогда, когда MS-DOS позволяет повторное вхождение. Кроме опасности повторного вхождения в MS-DOS необходимо предотвращать повторное вхождение в TSR до ее завершения (то есть если TSR может прерваться запуском самой себя), переключение стека на один и тот же массив неизбежно приведет к ошибке.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. В чем заключается задача аудита клавиатуры?
2. Как реализовать аудит клавиатуры в ОС MS-DOS?
3. Какие проблемы возникают при записи информации в файл аудита?
4. Что такое реентерабельность?
5. Какие способы обхода повторного вхождения в MS-DOS и в обработчик прерывания Вы знаете?

Лабораторная работа №8 Ассиметричные алгоритмы шифрования данных

Цель работы: освоить методику работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для дешифрования.

Задание:

1. Разработать консольное приложение для шифрования/дешифрования произвольных файлов с помощью алгоритма RSA.
2. Разработать визуальное приложение для шифрования/дешифрования изображений.

Порядок выполнения:

В приложении предусмотреть выполнение алгоритма RSA:

1. Вычисление ключей
2. Шифрование
3. Дешифрование

Форма отчетности: **Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Алгоритм функционирования программы в фоновом режиме.
5. Выводы

Задания для самостоятельной работы: Проанализировать проделанную работу с целью выявления недостатков алгоритма.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Алгоритм RSA разработан в 1977 г. Роном Ривестом, Ади Шамиром и Леном Адлеманом и опубликован в 1978 г. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм RSA:

1. Вычисление ключей

Важным моментом в этом криптоалгоритме является создание пары ключей: открытого и закрытого. Для алгоритма RSA этап создания ключей состоит из следующих операций:

1.1. Выбираются два простых различных числа p и q. Вычисляется их произведение n = p · q, называемое модулем. Под простым числом будем понимать такое число, которое делится только на 1 и на само себя. Взаимно простыми числами будем называть такие числа, которые не имеют ни одного общего делителя, кроме единицы.

1.2. Вычисляется функция Эйлера Φ(n) = (p – 1) · (q – 1).

1.3. Выбирается произвольное число e (e < n), такое, что 1 < e < Φ(n) и не имеет общих делителей, кроме 1 (взаимно простое) с числом (p – 1) · (q – 1).

1.4. Вычисляется d методом Евклида таким образом, что (e · d – 1) делится на (p – 1) · (q – 1).

1.5. Два числа (e, n) публикуются как открытый ключ.

1.6. Число d хранится в секрете – закрытый ключ есть пара (d, n), который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

2. Шифрование

Шифрование с помощью пары чисел производится следующим образом:

2.1. Отправитель разбивает своё сообщение M на блоки mi. Значение mi < n, поэтому длина блока mi в битах не больше k = [log2(n)] бит, где квадратные скобки обозначают, взятие целой части от дробного числа.

Например, если n = 21, то максимальная длина блока k = [log2(21)] = [4.39…]= = 4 бита.

2.2. Подобный блок может быть интерпретирован как число из диапазона (0; 2k – 1). Для каждого такого числа mi вычисляется выражение (ci – зашифрованное сообщение): ci = ((mi)e) mod n.

Необходимо добавлять нулевые биты слева в двоичное представление блока c_i до размера k = [log2(n)] бит.

3. Дешифрование

Чтобы получить открытый текст, необходимо каждый блок дешифровать отдельно: mi = ((ci)d) mod n.

Пример:

Выбрать два простых числа: p = 7, q = 17.

Вычислить n = p · q = 7 · 17 = 119.

Вычислить Φ(n) = (p – 1) · (q – 1) = 96.

Выбрать e так, чтобы e было взаимнопростым с Φ(n) = 96 и меньше, чем Φ(n): e = 5.

Определить d так, чтобы d · e ≡ 1 mod 96 и d < 96, d = 77, так как

77 · 5 = 385 = 4 · 96 + 1.

Результирующие ключи открытый {5, 119} и закрытый ключ {77, 119}.

Например, требуется зашифровать сообщение M = 19: 195 = 66 (mod 119),

C = = 66. Для дешифрования вычисляется 6677 (mod 119) = 19.

8. Пользователь должен иметь возможность поменять пароль

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

2. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки

1. Дайте определение алгоритма с открытым ключом.
2. Сколько этапов содержит алгоритм RSA?
3. В чем заключается вычисление ключей алгоритма RSA?
4. Как происходит шифрование в алгоритме RSA?
5. Как происходит дешифрование в алгоритме RSA?

9.2. Методические указания по выполнению курсового проекта (курсовой работы), контрольной работы, РГР, реферата

не предусмотрено

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security.
ОС Linux
LibreOffice

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия (*Лк, Лр , кр)*	***Наименование аудитории***	***Перечень основного оборудования***	***№ Лр***
1	**3**	**4**	**5**
Лк	Лекционная аудитория	-	№ 1.1 -3.2
ЛР	Лаборатория параллельных вычислений	Оборудование 14-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1-5
СР	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ОПК-2	способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии	**1**. Структура теории компьютерной безопасности.	1.1. Основные понятия теории компьютерной безопасности.	Индивидуальное задание Вопрос к зачету 1-2
			1.2. Методология построения защищенных автоматизированных систем.	Индивидуальное задание Вопрос к зачету 3- 4
		2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	2.1.Политика безопасности.	Индивидуальное задание Вопрос к зачету 5-6
			2.2.Стандарты в области информационной безопасности.	Индивидуальное задание Вопрос к зачету 7 - 8
ПК-5	целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках.	**1**. Структура теории компьютерной безопасности.	1.1.Основные понятия теории компьютерной безопасности.	Индивидуальное задание Вопрос к зачету 9
			1.2. Методология построения защищенных автоматизированных систем.	Индивидуальное задание Вопрос к зачету 10
		2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	2.1. Политика безопасности.	Индивидуальное задание Вопрос к зачету 11 - 13
			2.2 Стандарты в области информационной безопасности.	Индивидуальное задание Вопрос к зачету 14 - 16

2.Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ОПК-2	способностью приобретать новые научные и профессиональные зна-	**1.**Анализ угроз информационной безопасности.	**1.** Структура теории компьютер-
			2.Модели ценности информации.	

		ния, используя современные образовательные и информационные технологии	**3.**Построение систем защиты от угрозы нарушения конфиденциальности информации.	ной безопасности.
			4.Построение систем защиты от угрозы нарушения целостности информации.	
			5.Модель безопасности Харрисона-Руззо-Ульмана, распространение прав доступа.	**2.** Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.
			6.Модель безопасности Белла-Лападулы, распространение прав доступа.	
			7.Стандарт оценки безопасности компьютерных систем TCSEC.	
			8.Стандарт оценки безопасности компьютерных систем Гостехкомиссии РФ.	
2.	ПК-5	способность осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках.	**9**.Основные понятия теории компьютерной безопасности.	**1.** Структура теории компьютерной безопасности.
			10.Реализация парольной защиты.	
			11.Политика безопасности.	**2.** Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.
			12.Мандатная политика разграничения доступа.	
			13.Единые критерии безопасности информационных технологий.	
			14.Ценность информации.	
			15.Построение системы защиты от угрозы раскрытия параметров информационной системы.	
			16.Классификация защищенности ОС семейства *Nix.	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
нать (ОПК-2) – современные образовательные и информационные технологии, информационные системы и ресурсы; (ПК-5) - различные типы информации, которые можно извлекать из сети Интернет **Уметь** (ОПК-2) – находить, классифицировать и использовать информационные интернет- технологии, базы данных, webресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний; (ПК-5) приобретать новые научные и профессиональные знания, используя современные технологии поиска информации в глобальных компьютерных сетях **Владеть** (ОПК-2) – знаниями в области современных технологий, баз данных, webресурсов, специализированного программного обеспечения и т.п. и их практическим применением; (ПК-5) - навыками осуществлять целенаправленный поиск информации о научных и технологических достижениях в сети Интернет.	**Зачтено**	Демонстрирует все показатели на высоком уровне. Обучающийся всесторонне и глубоко владеет знаниями, сложными навыками, способен уверенно ориентироваться в практических ситуациях. Достигнут высокий уровень формирования компетенций.
	Не зачтено	Демонстрирует основную часть показателей на достаточном уровне. Обучающийся частично проявляет знания и навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается. Достигнут только базовый уровень формирования компетенции.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина Теоретические основы информационной безопасности направлена на ознакомление с основами организации информационной безопасности; на получение теоретических знаний и практических навыков в области организации мер по созданию систем защиты информации для их дальнейшего использования в практической деятельности.

Изучение дисциплины Теоретические основы информационной безопасности предусматривает:

- лекции,
- лабораторные работы;
- самостоятельную работу студентов;
- зачет.

В ходе освоения раздела 1 Структура теории компьютерной безопасности, студенты должны уяснить основные понятия теории компьютерной безопасности, методологию построения защищенных автоматизированных систем.

В ходе освоения раздела 2 Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем, студенты должны уяснить положения политики безопасности, специфику и разновидности стандартов в области информационной безопасности.

Необходимо овладеть навыками и умениями применения изученных методов для организации информационной безопасности, применения и реализации тех или иных проектов в конкретных ситуациях.

При подготовке к зачету рекомендуется особое внимание уделить следующим вопросам: модель безопасности Харрисона-Руззо-Ульмана, распространение прав доступа; модель безопасности Белла-Лападулы, распространение прав доступа; стандарт оценки безопасности компьютерных систем TCSEC; стандарт оценки безопасности компьютерных систем Гостехкомиссии РФ.

В процессе проведения лабораторных работ происходит закрепление знаний, формирование умений и навыков реализации представления об организации и политике информационной безопасности.

Самостоятельную работу необходимо начинать с изучения рекомендуемой литературы.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

Предусмотрено проведение аудиторных занятий (в виде лекций, лабораторных работ) в сочетании с внеаудиторной работой.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Теоретические основы информационной безопасности

1. Цель и задачи дисциплины

Целью изучения дисциплины является: Освоение студентами принципов и методов защиты информации, комплексного проектирования и анализа защищенных автоматизированных систем. Развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства и информационной инфраструктуры общества и государства.

Обеспечение бакалавров опорными знаниями для выполнения научно-исследовательских работ и практических работ, связанных с широким набором вопросов защиты информации и организации систем информационной безопасности.

Задачи дисциплины: сформировать понятия о вопросах:

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- процесса сбора, передачи, накопления и обработки информации;
- методов и средств ведения информационных войн;
- оценки защищенности и обеспечения информационной безопасности объектов информатизации.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-17 час., ЛР-34 час.; СР-57 час.

Общая трудоемкость дисциплины составляет 108 часа, 3 зачетных единиц

2.2 Основные разделы дисциплины:

1. Структура теории компьютерной безопасности.
2.Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-2- способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии

ПК-5- способность осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках.

4. Виды промежуточной аттестации: зачет.

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:

_____

_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____

_____

_____

Протокол заседания кафедры №____ от «___» _____ 20 ____ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ОПК-2	способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии	**1**. Структура теории компьютерной безопасности.	1.1. Основные понятия теории компьютерной безопасности.	Индивидуальное задание Отчет по ЛР
			1.2. Методология построения защищенных автоматизированных систем.	Индивидуальное задание Отчет по ЛР
		2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	2.1.Политика безопасности.	Индивидуальное задание Отчет по ЛР
			2.2.Стандарты в области информационной безопасности.	Индивидуальное задание Отчет по ЛР
ПК-5	целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках.	**1**. Структура теории компьютерной безопасности.	1.1.Основные понятия теории компьютерной безопасности.	Индивидуальное задание Отчет по ЛР
			1.2. Методология построения защищенных автоматизированных систем.	Индивидуальное задание Отчет по ЛР
		2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	2.1. Политика безопасности.	Индивидуальное задание Отчет по ЛР
			2.2 Стандарты в области информационной безопасности.	Индивидуальное задание Отчет по ЛР

2. Описание показателей и критериев оценивания компетенций

Так как текущий контроль проводится в форме тестирования и предназначен для проверки знаний самими обучающимися, тест может быть зачтен или не зачтен. В дальнейшем студенты могут повторить попытки выполнить тест по той теме, где были обнаружены пробелы в его знаниях.

Показатели	Оценка	Критерии
Знать (ОПК-2) – современные образовательные и информационные технологии, информационные системы и ресурсы; (ПК-5) - различные типы информации, которые можно извлекать из сети Интернет **Уметь** (ОПК-2) – находить, классифицировать и использовать информационные интернет- технологии, базы данных, webресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний; (ПК-5) приобретать новые научные и профессиональные знания, используя современные технологии поиска информации в глобальных компьютерных сетях **Владеть** (ОПК-2) – знаниями в области современных технологий, баз данных, webресурсов, специализированного программного обеспечения и т.п. и их практическим применением; (ПК-5) - навыками осуществлять целенаправленный поиск информации о научных и технологических достижениях в сети Интернет.	**Зачтено**	Демонстрирует более половины показателей на достаточном и высоком уровне
	Не зачтено	Демонстрирует большинство показателей на недостаточном и крайне низком уровне

Фонд тестовых заданий

по дисциплине

Б1.В.ДВ.09.01 Теоретические основы информационной безопасности

ТЕМАТИЧЕСКАЯ СТРУКТУРА ТЕСТОВ

N раздела	Наименование радела	N задания	Тема задания
1.	Структура теории компьютерной безопасности.	1-13	1.1. Основные понятия теории компьютерной безопасности.
			1.2. Методология построения защищенных автоматизированных систем..
2.	Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.	14-36	2.1. Политика безопасности.
			2.2 Стандарты в области информационной безопасности.

Тестовые задания

Задание № 1

Вопрос:

Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:

Выберите несколько из 6 вариантов ответа:

1) конфиденциальность

2) целостность

3) доступность

4) учет

5) неотрекаемость

6) мобильность

Задание № 2

Вопрос:

Сопоставьте понятия и их определения.

Укажите соответствие для всех 5 вариантов ответа:

1) возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями.

2) возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен.

3) возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.

4) все значимые действия лица, выполняемые им в рамках, контролирумых системой безопасности, должны быть зафиксированы и проанализированы.

5) лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.

__ конфиденциальность

__ целостность

__ доступность

__ учет

__ неотрекаемость

Задание № 3

Вопрос:

... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация

3) Аутентификация

4) Контроль доступа

5) Авторизация

Задание № 4

Вопрос:

... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация

3) Аутентификация

4) Контроль доступа

5) Авторизация

Задание № 5

Вопрос:

... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация

3) Аутентификация

4) Контроль доступа

5) Авторизация

Задание № 6

Вопрос:

... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация

3) Аутентификация

4) Контроль доступа

5) Авторизация

Задание № 7

Вопрос:

... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация

3) Аутентификация

4) Контроль доступа

5) Авторизация

Задание № 8

Вопрос:

... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты

2) Управление конфигурацией

3) Управление пользователями

4) Управление рисками

5) Обеспечение устойчивости

Задание № 9

Вопрос:

... - поддержание среды информационого обмена в минимально допустимом работоспособном состоянии и сооответствии требованиям информационной безопасности в услових деструктивны внешних или внутренних воздействий.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты

2) Управление конфигурацией

3) Управление пользователями

4) Управление рисками

5) Обеспечение устойчивости

Задание № 10

Вопрос:

... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационой безопасности.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты

2) Управление конфигурацией

3) Управление пользователями

4) Управление рисками

5) Обеспечение устойчивости

Задание № 11

Вопрос:

Перечислите основные направления информационной безопасности.

Выберите несколько из 4 вариантов ответа:

1) Физическая безопасность

2) Компьютерная безопасность

3) Визуальная безопасность

4) Сензитивная безопасность

Задание № 12

Вопрос:

Перечислите состав службы информационной безопасности.

Выберите несколько из 6 вариантов ответа:

1) Руководитель службы

2) Операционный отдел

3) Исследовательский отдел

4) Методический отдел

5) Отдел общения с прессой

6) Отдел бухгалтерии

Задание № 13

Вопрос:

Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это ...

Запишите ответ:

_____

Задание № 14

Вопрос:

Критериями определения уровня безопасности систем являются:

Выберите несколько из 5 вариантов ответа:

1) Оранжевая книга

2) Красная книга

3) Зеленая книга

4) Серо-буромалиновая книга

5) Белая книга

Задание № 15

Вопрос:

... - выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем.

Выберите один из 5 вариантов ответа:

1) Оранжевая книга

2) Красная книга

3) Белая книга

4) Зеленая книга

5) Открытая книга

Задание № 16

Вопрос:

... - выпущенные Министерством обороны США расширение критериев оценки уровня безопасности компьютерных систем для случаев использования компьютерных систем в информационной сети.

Выберите один из 5 вариантов ответа:

1) Оранжевая книга

2) Красная книга

3) Белая книга

4) Зеленая книга

5) Открытая книга

Задание № 17

Вопрос:

Перечислите модели классификации информационных объектов.

Выберите несколько из 5 вариантов ответа:

1) По наличию

2) По несанкционированной модификации (целостность)

3) По разглашению

4) По принадлежности

5) По аппелируемости

Задание № 18

Вопрос:

Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время.

Выберите один из 6 вариантов ответа:

1) критической

2) очень важной

3) важной

4) полезной

5) несущественной

6) вредной

Задание № 19

Вопрос:

Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы.

Выберите один из 6 вариантов ответа:

1) критической

2) очень важной

3) важной

4) полезной

5) несущественной

6) вредной

Задание № 20

Вопрос:

Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта.

Выберите один из 6 вариантов ответа:

1) критической

2) очень важной

3) важной

4) полезной

5) несущественной

6) вредной

Задание № 21

Вопрос:

Какой считается информация, по классификации информационных объектов, разглашение которой может принести моральный ущерб в очень редких случаях.

Выберите один из 6 вариантов ответа:

1) критической

2) очень важной

3) важной

4) значимой

5) малозначимой

6) незначимой

Задание № 22

Вопрос:

Какой считается информация, по классификации информационных объектов, если ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта, последствия модификации необратимы.

Выберите один из 6 вариантов ответа:

1) критической

2) очень важной

3) важной

4) значимой

5) малозначимой

6) незначимой

Задание № 23

Вопрос:

Жизненный цикл информации состоит из следующих стадий:

Выберите несколько из 4 вариантов ответа:

1) Информация используется в операционном режиме

2) Информация используется в архивном режиме

3) Информация хранится в архивном режиме

4) Информация хранится в операционном режиме

Задание № 24

Вопрос:

Какие существуют основные классы атак?

Выберите несколько из 5 вариантов ответа:

1) Локальная атака

2) Удаленная атака

3) Атака на поток данных

4) Атака фрикера

5) Распределенная атака

Задание № 25

Вопрос:

... - это случай, когда злоумышленник оказался непосредственно перед клавиатурой данного компьютера

Выберите один из 5 вариантов ответа:

1) Локальная атака

2) Удаленная атака

3) Атака на поток данных

4) Распределенная атака

5) Атака фрикера

Задание № 26

Вопрос:

... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает.

Выберите один из 5 вариантов ответа:

1) Локальная атака

2) Удаленная атака

3) Атака на поток данных

4) Рейдерская атака

5) Социальная инженерия

Задание № 27

Вопрос:

... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами.

Выберите один из 5 вариантов ответа:

1) Локальная атака

2) Удаленная атака

3) Атака на поток данных

4) Рейдерская атака

5) Социальная инженерия

Задание № 28

Вопрос:

... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности.

Выберите один из 5 вариантов ответа:

1) Хакер

2) Кракер

3) Фрикер

4) Джокер

5) Анонимайзер

Задание № 29

Вопрос:

... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес.

Выберите один из 5 вариантов ответа:

1) Хакер

2) Кракер

3) Фрикер

4) Джокер

5) Анонимайзер

Задание № 30

Вопрос:

... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах.

Выберите один из 5 вариантов ответа:

1) Хакер

2) Кракер

3) Фрикер

4) Джокер

5) Анонимайзер

Задание № 31

Вопрос:

... - это набор мероприятий по сбору сведений об информационной системе, напрямую не связанный с техническими подробностями реализации системы, основанный на человеческом факторе.

Запишите ответ:

_____

Задание № 32

Вопрос:

... в аппаратном обеспечении -это устройство, которое выполняет некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы.

Запишите ответ:

_____

Задание № 33

Вопрос:

... - это устройство, хранящее некий уникальный параметр, на основе которого выдается корректный ответ на запрос системы об аутентификации.

Выберите один из 4 вариантов ответа:

1) Токен

2) Пароль

3) Биометрические параметры

4) Мастер-ключ

Задание № 34

Вопрос:

Выполнение пользователем, получившим дюступ в систему, различных несанкционированных действий, называется атакой на ...

Запишите ответ:

_____

Задание № 35

Вопрос:

... - это программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, котрое станция при нормальной работе должна проигнорировать.

Запишите ответ:

_____

Задание № 36

Вопрос:

... позволяют провести анализ и пошаговое выполнение программного обеспечения с тем, чтобы понять его внутреннюю логику и уязвимость или вызвать в его работе сбой с предсказуемым результатом, либо изменить ход работы программы в свою пользу.

Выберите один из 4 вариантов ответа:

1) Дизассемблеры

2) Программы повышения прав

3) Атаки на переполнение буфера

4) Программы подбора паролей

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика от «12» марта 2015 г. №228

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015 г. №475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06»июня 2016 г. №429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. №125

для набора 2018 года и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018 г. №130

Программу составил:

Сташок О.В. к.т.н, доцент каф. математики и физики _____

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и физики

от «21» ноября 2018 г., протокол № 3

Заведующий кафедрой
Математики и физики _____ О.И.Медведева

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой МиФ _____ О.И Медведева

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4
Председатель методической комиссии факультета _____ М.А. Варданян

СОГЛАСОВАНО:
Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____

(методический отдел)