Приложение к РПД

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

по учебной дисциплине

«Технологии защиты информации»

для направления подготовки/специальности 44.04.01 Педагогическое образование

Направленность программы: Магистерская программа «Информационные технологии в физико-математическим образовании»

1. Описание показателей (дескрипторов) и критериев оценивания компетенций на различных этапах их формирования

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

ОПК-1 Способен осуществлять и оптимизировать профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики
ПК-2 Способен анализировать и систематизировать результаты научных и научно-методических исследований, а также проводить исследования в области физико-математического образования

Компетенции	Показатели* (дескрипторы)	Критерии в соответствии с уровнем освоения ОП			Оценочное средство (промежуточная аттестация)
		пороговый (удовлетворительно) 55-69 баллов	стандартный (хорошо) 70-84 балла	эталонный (отлично) 85-100 баллов	

ОПК-1	Знать	основные понятия информационной безопасности	критерии оценки защищенности систем; терминологическую систему информационной безопасности	правовые основы защиты информации (основные положения законодательных актов, регламентирующие правовые аспекты информационной безопасности).	Итоговое тестирование
	Уметь	излагать основные концепции информационной безопасности	работать с программным обеспечением, обеспечивающим защиту информации в компьютерных сетях	эффективно использовать полученные знания в области нормативно-правовых актов и современных компьютерных технологий и пакетов прикладных программ для решения задач информационной безопасности	Доклад, конспект, рефера
	Владеть	умением демонстрировать понимание основных правовых норм, понятий, принципов, закономерностей и концепций информационной безопасности	умением выбирать наиболее оптимальные программные и аппаратные решения для защиты ПК и компьютерных сетей	действиями по соблюдению правовых норм и умением использовать возможности информационных технологий для решения задач информационной безопасности.	Доклад, конспект, реферат
ПК-2	Знать	основные проблемы и направления развития аппаратных и программных средств защиты информации в сетях.	актуальные проблемы и направления развития аппаратных и программных средств защиты информации в сетях.	фундаментальные концепции информационной безопасности, необходимые для проведения исследований в профессиональной области.	Итоговое тестирование
	Уметь	оценивать собственные образовательные достижения и проблемы, определять потребности в дальнейшем образовании	самостоятельно получать и расширять знания, пользоваться различными источниками информации	решать исследовательские задачи в области информационной безопасности, проектировать пути своего профессионального развития	Лаб. работы
	Владеть	способностью к работе в команде, выполнению проектной деятельности	навыками проведения проектной работы в рамках учебной информации.	методами самостоятельного получения и расширения знаний, умением пользоваться различными источниками информации, навыками проектной работы в профессиональной области.	Лаб. работы

*Показатели (дескрипторы) перечисляются по всей компетенции, если индикаторы компетенции сформулированы в виде «действия».

2. Описание критериев и шкал оценивания результатов обучения по дисциплине

2.1. Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях. Контролируемые разделы (темы) дисциплины, компетенции и оценочные средства представлены в таблице.

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции и/или индикаторы компетенции	Наименование оценочного средства**
1	Технологии защиты информации	ОПК-1	Доклад Реферат Конспект
		ПК-2	Лабораторные работы
2	Криптография	ОПК-1	Доклад Реферат Конспект
		ПК-2	Лабораторные работы
3	Защита информации	ОПК-1	Доклад Реферат Конспект
		ПК-2	Лабораторные работы
4	Вредоносное ПО	ОПК-1	Доклад Реферат Конспект Итоговое тестирование
		ПК-2	Лабораторные работы Итоговое тестирование

** Наименование темы (раздела) или тем (разделов) берется из рабочей программы дисциплины.*

*** Примеры процедур оценивания: тестирование, контрольная работа, эссе, реферат, коллоквиум, выполнение кейса, решение ситуационных задач, написание диктанта и т.д.*

Критерии и шкала оценивания лабораторных работ

Объем правильно выполненной работы и уровень допущенных ошибок	2 балла
Использование изученных алгоритмов и средств защиты для решения задачи	2 балла
Умение выбрать наиболее подходящий программный инструментарий для решения конкретных профессиональных задач	2 балла
Умение использовать различные современные информационные технологии и пакеты прикладных программ для решения поставленных задач	2 балла
Максимальный балл	8 баллов

Критерии и шкала оценивания конспекта по теме

Умение проводить смысловую группировку текста, выделять основополагающие идеи	2 балла
Умение высказывать оценочные суждения, свою точку зрения о прочитанном тексте	2 балла
Максимальный балл	4 балла

Критерии и шкала оценивания доклада по теме

Содержательность сообщения и убедительность приводимых аргументов	1 балл
Опора на научные теории и концепции в обосновании отбора содержания доклада	1 балл
Умение ответить на вопросы слушателей по теме доклада	1 балл
Наличие практических примеров в докладе	2 балла
Максимальный балл	5 баллов

Критерии и шкала оценивания реферата

Понимание проблемы, стремление разъяснить ее суть с научных позиций	2 балла
Умение интересно подать материал, наличие личностного отношения к нему	1 балл
Содержание подкреплено необходимыми комментариями, примерами и поясняющими цитатами	2 балла
Максимальный балл	5 баллов

Критерии и шкала оценивания итогового контрольного теста

Оценка	Критерий оценки
0 баллов	менее 40% правильных ответов из общего числа предъявленных заданий
7 баллов	от 41% до 55% правильных ответов из общего числа предъявленных заданий
8 баллов	от 56% до 70% правильных ответов из общего числа предъявленных заданий
10 баллов	от 71% до 85% правильных ответов из общего числа предъявленных заданий
12 баллов	от 86% до 100% правильных ответов из общего числа предъявленных заданий

Итоговое тестирование

Итоговый тест включает в себя задания с выбором ответа, позволяющие оценить знание программного материла дисциплины. Максимальное число баллов – 12.

2.2. Критерии и шкалы оценивания результатов обучения при проведении промежуточной аттестации

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется двухбалльная шкала

Основные виды систем оценивания

Европейская	100-балльная	4-балльная	2-балльная
A	94-100	отлично	зачтено
A-	90-94		
B+	85-89		
B	80-84	хорошо	
B-	75-79		
C+	70-74		
C	65-69	удовлетворительно	
C-	60-64		
D	55-59		
F	50-54	неудовлетворительно	не зачтено

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется двухбалльная шкала: «зачтено», «не зачтено».

Шкала оценивания	*Критерии оценивания*	*Уровень освоения компетенций*
«зачтено»	*Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Ответил на все дополнительные вопросы*	*Эталонный*
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Ответил на большинство дополнительных вопросов	*Стандартный*
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Допустил много неточностей при ответе на дополнительные вопросы	*Пороговый*
«не зачтено»	*Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений. При ответах на дополнительные вопросы было допущено множество неправильных ответов*	*Компетенции не сформированы*

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта

деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Оценочные средства текущего контроля успеваемости

Задания для конспекта

Модуль 1.

Правовые основы защиты информации.

Модуль 2.

Методы криптографического преобразования данных.

Модуль 3. Особенности защиты информации в ПК.

Модуль 4. Сервисы безопасности в компьютерных сетях.

Темы для докладов

Модуль 1.

Обнаружение скрытых процессов и вирусов в ПК. Работа с программами, позволяющими обнаружить скрытые процессы.

Модуль 2.

Способы шифрования электронных сообщений. Работа с программой gpg (получение открытого и закрытого ключей, шифровка и расшифровка сообщения).

Модуль 3.

Пароли и учетные записи пользователей в средах Windows, локальные политики безопасности.

Модуль 4.

Обнаружение нарушений в сети, раскрыть критерии оценки защищенности компьютерных систем.

Темы для реферата

Модуль 1.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Модуль 2.

Типы криптографических услуг. Защита авторских прав.

Модуль 3.

Структура системы защиты от несанкционированного копирования.

Модуль 4.

Механизмы заражения компьютерными вирусами.

Практические работы

Модуль 1.

Лабораторная работа №1

Изучить статьи 272, 273, 274 УК РФ

Изучить Гражданский кодекс часть IV (авторское право, имущественное право, исключительное право)

Модуль 2.

Лабораторная работа №2

Работа с программой GPG

gpg --version

Симметричное шифрование

Ситуация, когда у вас есть секретный пароль, который вы используете, для того чтобы зашифровать и расшифровать файл, называется симметричным шифрованием. Им пользоваться проще всего.

Зашифровать файл:

gpg -c filename

Расшифровать файл:

gpg --decrypt-files filename.gpg

В обоих случаях программа попросит вас ввести пароль. К названию зашифрованного файла добавляется расширение .gpg. По умолчанию gpg также компрессирует файлы, которые шифрует.

Ассиметричное шифрование

Ассиметричное шифрование сложнее, но именно им обычно и пользуются, когда работают с gpg.

Слабым моментом симметричного шифрования является то, что когда вы посылаете зашифрованный файл, вам надо каким-то образом передать получателю и секретный пароль.

Ассиметричное шифрование решает эту проблему весьма элегантным образом. Вместо одного пароля вы используете два. Один - публичный, который вы активно раздаёте всем желающим, второй - ваш личный секретный пароль, который знаете только вы. Когда вам хотят послать что-нибудь секретное, отправитель шифрует это посредством публичного пароля. А вы уже со своей стороны расшифровываете полученный файл своим личным паролем. Ваш секретный пароль при этом никуда не передаётся и не может попасть в чужие руки.

Пароли и ключи

Итак, вам нужна пара паролей, или как их ещё называют, ключей. Одним паролем шифруют, другим расшифровывают. Они создаются автоматически. Ключи - скорее куски текста, содержащие набор символов.

Ключи хранятся в специальной копилке, добавлять и удалять их оттуда можно с помощью программы gpg. Создавать ключи тоже.

Создание пары ключей

Чтобы создать свою собственную пару ключей запустите следующую команду:

gpg --gen-key.

Программа предлагает разумные параметры по умолчанию, соглашайтесь с тем, что предлагает gpg, укажите только своё имя и e-mail.

Созданные ключи не сохраняются в файл, а попадают в копилку ключей. Убедиться в этом можно набрав команду

gpg --list-keys.

Ключ:

pub 1024D/0443FB22 2008-06-02

uid Anton

sub 2048g/5F28F4F0 2008-06-02

0443FB22 в первой строчке, это id ключа. Если вы впоследствии захотите обратиться к ключу в коллекции, то вам придётся указать либо его id, либо какую-нибудь часть записи, которая позволит эго однозначно идентифицировать.

Экспорт и импорт ключей

Теперь экспортируем только что созданный ключ в текстовый файл. После этого вы можете его разослать своим друзьям, и начинать обмениваться секретной информацией.

Следующая команда экспортирует публичный ключ:

gpg --output mygpgkey_pub.txt --armor --export 0443FB22

mygpgkey_pub.txt - название файла, куда будет сохранён ключ; --armor значит, что файл будет текстовым (по умолчанию создаётся бинарный).

Вместо id можно использовать имя или e-mail как полностью, так и частично. Например, команды

gpg --output mygpgkey_pub.txt --armor --export Anton

или

gpg --output mygpgkey_pub.txt --armor --export anton@mail.ru

делают то же самое.

Если вам нужно перенести свой личный ключ на другой компьютер - скажем, чтобы использовать тот же самый ключ на нескольких машинах, сделать это можно так:

gpg --output mygpgkey_sec.txt --armor --export-secret-key Anton

Чтобы импортировать ключи используйте следующие команды:

gpg --import mygpgkey_pub.txt

gpg --allow-secret-key-import --import mygpgkey_sec.txt

Вопрос: ваш друг прислал вам свой публичный ключ. Как его добавить в коллекцию ключей на вашей машине?

Если вы читали внимательно, вы скажете: gpg --import filename.txt, и будете правы, но чтобы пользоваться ключом, вам ещё специфически надо указать, что вы доверяете владельцу этого ключа.

Найдите ключ, который вы импортировали (gpg --list-keys). Дальше наберите gpg --edit-key Anton (используйте имя владельца, или id ключа). Откроется шелл клиент для редактирования ключа, куда вы сможете вбивать разные команды. Напишите trust <Enter>, из списка выберите «5 = I trust ultimately», написав 5 <Enter> . Потом quit <Enter>, чтобы выйти. Вот теперь уже импортированным ключом можно пользоваться.

Шифрование

gpg --recipient Anton --encrypt filename

--recipient - для кого шифруем (id публичного ключа, имя или e-mail адрес, которые позволяют выбрать ключ из копилки). По умолчанию к filename добавляется расширение .gpg. Если вы хотите задать другое имя файла, добавьте к команде --output another_filename.gpg.

В результате файл будет зашифрован. В обычной ситуации никто, кроме получателя, не сможет его расшифровать. Но сейчас мы просто тестируем и вы одновременно являетесь и получателем и отправителем, так что теперь вы можете расшифровать файл, используя следующую команду:

gpg --decrypt-files filename.gpg

Обратите внимание, что это не --decrypt, а --decrypt-files. Просто --decrypt печатает результат в окно, где бежит ваша командная строка, а это не то, что вы хотите. Gpg спросит ещё ваш секретный пароль, который вы указали, когда создавали ключ.

Цифровые подписи и их проверка

Цифровая подпись удостоверяет создателя и дату создания документа. Если документ будет каким-либо образом изменен, то проверка цифровой подписи будет неудачной. Цифровая подпись может использоваться в тех же целях, что и обычная подпись. Создание и проверка подписей отличается от зашифрования/расшифрования. При подписи документа используется закрытый ключ подписывающего, а проверяется подпись с использованием его открытого ключа. Для подписи документов используется команда −−sign.

gpg --output doc.sig --sign doc

Если не указать подписываемый документ, то данные считываются со стандартного ввода. Перед подписью документ сжимается. Подписанный документ выводится в двоичном формате.

Имея подписанный документ, Вы можете либо только проверить подпись, либо проверить подпись и восстановить исходный документ. Для проверки подписи используется команда −−verify. Для проверки подписи и извлечения документа используется команда −−decrypt.

gpg --output doc --decrypt doc.sig

Прозрачно подписанные(Clearsigned) документы

Обычно цифровые подписи применяются при подписи сообщений usenet и e-mail. При этом нежелательно сжимать подписываемые документы. Команда −−clearsign добавляет к документу цифровую подпись в формате ASCII, не изменяя при этом сам документ.

gpg --output doc.asc --clearsign doc

Отделённая подпись

Применение подписанных документов ограниченно. Получатель должен восстанавливать документ из подписанной версии, и даже в случае прозрачной подписи, подписанный документ должен быть отредактирован для получения оригинала. Поэтому имеется третий метод подписи документов, который создает отделённую подпись (detached signature). Отделённая подпись создается при использовании команды −−detach-sign.

gpg --output doc.sig --detach-sign doc

Для проверки подписи необходимы и подпись, и сам документ. Для проверки используется команда −−verify.

Модуль 3.

Лабораторная работа №3

Службы Windows, влияющие на безопасность

Службы (Services) - это приложения, запускаемые в фоновом режиме во время загрузки системы или при возникновении определенных событий и обеспечивающие основные функциональные возможности ОС. Как правило, службы не имеют графического интерфейса, поэтому их работа в большинстве своем не заметна для пользователя.

При стандартной установке Windows XP Professional в систему инсталлируется порядка 80-ти разнообразных служб. И, несмотря на то, что не все из них запускаются автоматически, количество работающих по умолчанию всё равно кажется слишком завышенным, если учесть, что значительная часть от общего числа уязвимостей, когда-либо обнаруженных в этой ОС, приходится именно на системные службы. К тому же, в домашних условиях во многих работающих по умолчанию службах просто нет никакой необходимости.

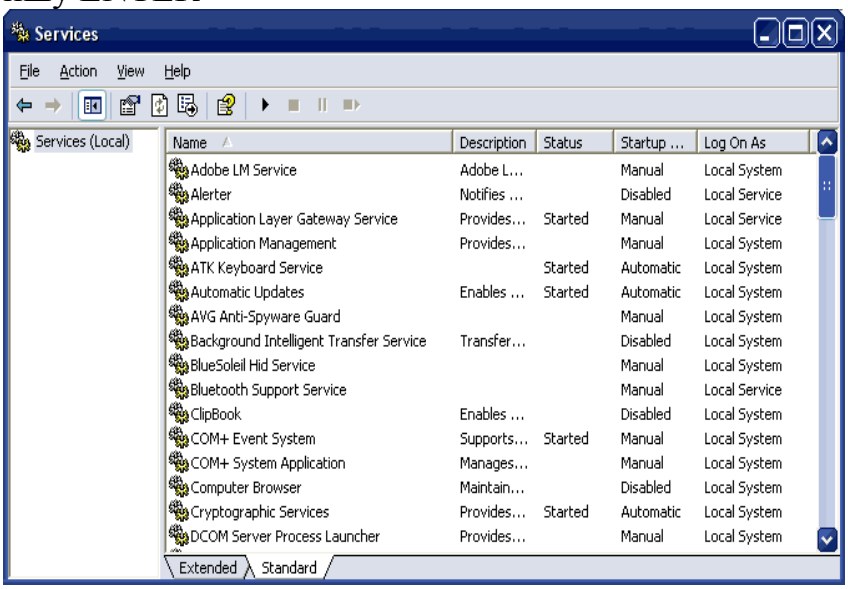
По этим и ряду других причин, связанных с оптимизацией работы компьютера, все неиспользуемые вами службы рекомендуется отключить. Более того, отключение ненужных служб и функций - один из эффективнейших способов защиты от возможных нападений.

Просмотреть список всех служб, установленных на компьютере, можно следующим образом:

Пуск\Панель Управления\Администрирование\Службы (Services)

Либо запустив из командной строки services.msc:

Пуск\Выполнить\ копируем в строку: services.msc\ нажимаем ОК или клавишу ENTER



Список установленных на компьютере служб

Эта консоль, помимо просмотра текущего состояния и описания всех служб, позволяет остановить, возобновить или отключить каждую из них, задать действия по восстановлению на случай сбоя, выполнить настройку для конкретного профиля оборудования, изменить тип запуска и многое другое.

Но нас, в первую очередь, будет интересовать последняя из перечисленных возможностей.

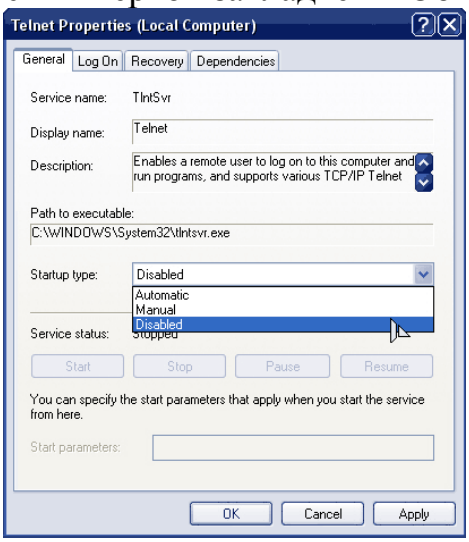
Итак, для каждой службы существует три варианта запуска:

Авто (Automatic) - служба запускается автоматически во время загрузки ОС;

Вручную (Manual) - служба запускается автоматически, в том случае, когда какой-либо процесс вызывает функцию StartService;

Отключено (Disabled) - служба не может быть запущена - попытки запустить службу закончатся неудачей.

Чтобы изменить значение типа запуска, установленное по умолчанию, кликните по нужной службе двойным нажатием мыши и в открывшемся окне свойств в первой закладке – «Общие» - выберите желаемый «Тип Запуска».



Изменение «Типа Запуска» службы

Ниже приведен основной список служб в алфавитном порядке, для которых «Тип Запуска» рекомендуется установить в положение «Отключено» (однако в качестве общего правила нужно принять, что необходимо отключить все неиспользуемое!):

Беспроводная настройка (Wireless Zero Configuration) - отключаем за полной ненадобностью в том случае, если вы не используете беспроводной интернет, и у вас нет адаптеров беспроводной связи, и вы не собираетесь использовать «нулевую» конфигурацию беспроводной сети.

Веб-клиент (WebClient) - позволяет приложениям Windows создавать, сохранять и изменять файлы, находящиеся на серверах WebDAV (использование Web Publishing Wizard для публикации данных в Интернет).

На просмотр ресурсов в Интернете отключение этой службы никак не влияет, поскольку она используется только для WebDAV-подключений, к тому же программы, которым этот сетевой протокол необходим, как правило, имеют встроенные перенаправители WebDAV, работающие независимо от службы «Веб-клиент».

Диспетчер очереди печати (Print Spooler) - отвечает за обработку, планирование и распределение документов, предназначенных для печати. Обязательно отключаем в том случае, если у вас нет принтера.

Диспетчер сеанса справки для удаленного рабочего стола (Remote Desktop Help Session Manager) - управляет возможностями удаленного помощника. Отключите, если не используете эту функцию.

Диспетчер сетевого DDE (Network DDE DSDM) - управляет общими ресурсами сетевого динамического обмена данными (DDE). По сути, DDE - это давно устаревшая и редко где используемая технология.

Маршрутизация и удаленный доступ (Routing and Remote Access) - обеспечивает многопротокольные функции маршрутизации, подключения удаленного доступа и удаленного доступа по сети VPN.

Модуль поддержки NetBIOS через TCP/IP (TCP/IP NetBIOS Helper Service) - данная служба необходима при совместном использовании ресурсов (между несколькими компьютерами) и для сетевой печати. Отключите, если у вас нет необходимости в этих функциях.

Обозреватель компьютера (Computer Browser) - обеспечивает функционирование списка Windows-доменов, компьютеров в масштабе всей сети и других аппаратных устройств, совместимых с протоколом NetBIOS. Для обычных пользователей и домашних компьютеров эта служба полностью бесполезна.

Оповещатель (Alerter) - посылает выбранным пользователям и компьютерам административные оповещения. В домашних условиях служба не нужна.

Планировщик заданий (Task Scheduler) - позволяет составлять расписание и автоматически запускать различные приложения, программы, скрипты, функцию резервного копирования и пр. в запланированное вами время (по умолчанию эти задания находятся здесь: WINDOWS\Tasks. Либо: Пуск\Программы\Стандартные\Служебные\Назначенные задания):

Если вы не используете эту функцию (.job-файлы), отключите эту службу (MS04-022; используется некоторыми вирусами для автозагрузки, пример: Trojan.Bookmarker.C).

Но также имейте в виду, что если у вас установлен ативирус Symantec или McAfee, то отключать эту службу не стоит. Так как эти программы

используют её для обновления в определенное время и запланированных сканирований системы.

Сервер (Server) - выполняет основные функции сервера: обеспечивает совместное использование файлов, принтеров, именованных каналов в сети. Если у вас нет необходимости открывать доступ к вашим файлам и принтерам, обязательно отключаем.

Сервер папки обмена (ClipBook) - позволяет просматривать содержимое папки буфера обмена удаленным пользователям. Просмоторщик буфера обмена (ClipBook Viewer) открывается следующим образом: Пуск\Программы\Стандартные\Окно папки обмена (ClipBook Viewer); либо в верхнем меню программы Acrobat Reader: Window\Clipboard Viewer. Если вы не хотите ни с кем обмениваться этой информацией, то отключите данную службу.

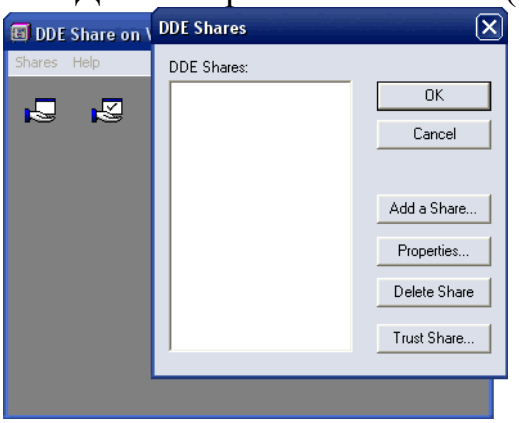
Сетевой вход в систему (Net Logon) - данная служба обеспечивает безопасность проверки подлинности пользователя при подключении его компьютера к домену. Если ваш компьютер не входит в домен, отключите её.

Служба индексирования (Indexing Service) - индексирует содержимое и свойства файлов на локальном и удаленных компьютерах, что позволяет производить поиск любого слова или фразы, которые содержатся в документах пользователя. Обычный поиск файлов после отключения этой службы не замедляется.

Служба обнаружения SSDP (SSDP Discovery Service) - выполняет поиск устройств UPnP в домашней сети. Обязательно отключаем в случае, если вы не работаете с сетевыми устройствами.

Служба сообщений (Messenger) - отправляет и получает сообщения, переданные администратором или службой оповещений. При отсутствии сети (и соответственно администратора) абсолютно бесполезна (никакого отношения к программе Windows/MSN Messenger, эта служба не имеет). Также желательно отключить для того, чтобы запретить net send сообщения для скрытия вашего компьютера от автоматизированных спам рассылок.

Служба сетевого DDE (Network DDE) - обеспечивает сетевой транспорт и безопасность для динамического обмена данными (DDE) для программ, выполняющихся на локальном или удаленных компьютерах. Аналогично службе «Диспетчер сетевого DDE» («Network DDE DSDM»).



Конфигурации DDE (%WINDIR%\system32\ddeshare.exe)

Службы терминалов (Terminal Services) - предоставляет возможность нескольким пользователям интерактивно подключаться к компьютеру, является основой для удаленного рабочего стола (включая удаленное администрирование), быстрого переключения пользователей и удаленного помощника.

Службы IPSEC (IPSEC Services) - данная служба обычно используется для шифрования IP-трафика между рабочей станцией и доменом, а также для VPN-соединений. Если вы не входите в домен и у вас нет VPN-сети, данную службу можно отключить.

Удаленный реестр (Remote Registry Service) - позволяет удаленным пользователям изменять параметры реестра на вашем компьютере (regedit\File\Connect Network Registry). Очень опасная служба.

Узел универсальных PnP-устройств (Universal Plug and Play Device Host) - обеспечивает поддержку и управление UPnP-устройствами. Предоставляет большие возможности удаленного поиска, но использует широковещательные пакеты. Отключите, если вы не подключаете к своей сети какие-либо UPnP-устройства.

NetMeeting Remote Desktop Sharing (NetMeeting Remote Desktop Sharing) - обеспечивает удаленный доступ соответствующим пользователям к рабочему столу Windows с других компьютеров с помощью программы Windows NetMeeting (программа NetMeeting предназначена для проведения аудио и видеоконференций в сети). Отключаем, если не используется.

Telnet (Telnet) - обеспечивает возможность соединения и удалённой работы в системе по протоколу Telnet (Teletype Network) с помощью командного интерпретатора. Не использует шифрование и поэтому очень уязвим для атак при применении его в сети.

Модуль 4.

Лабораторная работа №4

Скрытые процессы. Способы обнаружения

Эксплойт, эксплоит (англ. *exploit*, эксплуатировать) - это компьютерная программа, фрагмент программного кода или последовательность команд, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Классификация

В зависимости от метода получения доступа к уязвимому программному обеспечению, эксплойты подразделяются на удалённые (англ. *remote*) и локальные (англ. *local*).

Удалённый эксплойт работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;

Локальный эксплойт запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав суперпользователя.

Атака эксплойта может быть нацелена на различные компоненты вычислительной системы - серверные приложения, клиентские приложения или модули операционной системы. Для использования серверной уязвимости эксплойту достаточно сформировать и послать серверу запрос, содержащий вредоносный код. Использовать уязвимость клиента немного сложнее - требуется убедить пользователя в необходимости подключения к поддельному серверу (перехода по ссылке, в случае если уязвимый клиент является браузером).

Виды эксплойтов

Эксплойты, фактически, предназначены для выполнения сторонних действий на уязвимой системе и могут быть разделены между собой следующим образом:

Экслойты для операционных систем

Эксплойты для прикладного ПО (музыкальные проигрыватели, офисные пакеты и т. д.)

Эксплойты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие)

Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB)

Эксплойты для интернет-сайтов (facebook.com, livejournal.com)

Эксплойты в прошивке PSP

Другие эксплойты

Как выглядит эксплойт?

Эксплойт может распространяться в виде исходных текстов, исполняемых модулей, или словесного описания использования уязвимости. Он может быть написан на любом компилируемом или интерпретируемом языке программирования (наиболее частые: C/C++, Perl, PHP, HTML+JavaScript).

Эксплойты могут быть классифицированы также по типу используемой ими уязвимости, такой как: переполнение буфера, SQL-инъекция, межсайтовый скриптинг, подделка межсайтовых запросов и т. д.

Актуальность

Информация, полученная в результате обнаружения уязвимости, может быть использована как для написания эксплойта, так и для устранения уязвимости. Поэтому в ней одинаково заинтересованы обе стороны - и взломщик и производитель взламываемого программного обеспечения. Характер распространения этой информации определяет время, которое требуется разработчику до выпуска заплатки.

После закрытия уязвимости производителем шанс успешного применения эксплойта начинает стремительно уменьшаться. Поэтому особой популярностью среди хакеров пользуются так называемые 0-day эксплойты, использующие недавно появившиеся уязвимости, которые еще не стали известны общественности.

ROOTKIT

Само понятие изначально использовалось исключительно в мире UNIX, где под «Руткитом» подразумевали набор утилит, устанавливаемый на взломанном компьютере после получения прав суперпользователя, что впоследствии позволяло полностью скрыть следы какой-либо хакерской деятельности.

Суперпользователь или ROOT (отсюда и название) - это особый аккаунт в UNIX-системах, у владельца которого есть привилегии на выполнение всех без исключения операций.

В операционных системах Microsoft Windows под термином «RootKit» принято понимать программу или даже программный код, направленный на маскировку или сокрытие заданных объектов в системе.

Подобное осуществляется различными методами: в первую очередь с помощью перехвата базовых функций ОС, изменением содержимого системных таблиц процессора и модификаций системных структур операционной системы.

Т.е. благодаря руткиту можно скрыть всё, что позволило бы обнаружить на компьютере постороннее приложение: любые разделы реестра, процессы, папки и файлы, открытые порты TCP/UDP и т.д.

В качестве простого примера: перехват функции поиска файла на диске позволяет исключить маскируемые файлы из результатов этого поиска.

Также стоит заметить, что подобные технологии применяются не только вредоносными приложениями.

Системные процессы Windows

1.Userinit.exe

Userinit.exe является частью операционных систем Windows, отвечает за процесс загрузки системы. На нем лежит задача восстановления сетевых подключений и запуска оболочки.

Процесс является критическим для функционирования операционной системы. Не пытайтесь отключить его. Удаление файла приведет к невозможности загрузки операционной системы и потребует переустановку операционной системы.

2.services.exe

Service Control Manager. Обеспечивает создание, удаление, запуск и остановку сервисов ОС. Стартует при загрузке системы, обеспечивает работу службы Журнал событий, а также позволяет манипуляцию процессами удаленной машины

Функции

- Монтирование базы данных установленных сервисов.
- Запуск сервисов при загрузке операционной системы, либо по требованию.
- Получение количественной и качественной информации об установленных сервисах и системных драйверах.
- Пересылка управляющих запросов запущенным сервисам.
- Блокировка и разблокировка базы данных сервисо.в

Алгоритм работы

При загрузке операционной системы SCM запускает все сервисы, у которых указан тип запуска «Автоматически», а также все сервисы указанные в зависимостях автозапускаемых сервисов. Таким образом, при запуске сервиса с типом запуска «Автоматически», у которого в зависимостях указаны сервисы с типом запуска «Вручную», последние также будут запущены, несмотря на свой тип запуска.

После загрузки операционной системы пользователь может вручную запустить необходимые сервисы, воспользовавшись консолью управления сервисами.

Пользователь также может указать параметры запуска сервиса, которые будут переданы как аргументы функции StartService при запуске.

Во время запуска сервиса SCM выполняет следующие действия:

- Получение сохранённой в базе данных информации по учётной записи, с правами которой должен запускаться сервис.
- Авторизация под этой учётной записью.
- Получение пользовательского профиля.
- Подготовка процесса сервиса к выполнению.
- Привязка доступов учётной записи к порождённому процессу.
- Запуск процесса сервиса на выполнение.

3.lsass.exe

LSASS - часть операционной системы, отвечающей за авторизацию локальных пользователей отдельного компьютера (сокращение от Local Security Authority Subsystem Service). Сервис является критическим, так как без него вход в систему для локальных пользователей (не зарегистрированных в домене) невозможен в принципе.

Процесс проверяет данные для авторизации, при успешной авторизации служба выставляет флаг о возможности входа. Если авторизация была запущена пользователем, то также ставится флаг запуска пользовательской оболочки. Если авторизация была инициализирована службой или приложением, данному приложению предоставляются права данного пользователя.

При заражении троянской программой или при получении полного доступа к данному сервису система полностью «обезоруживается» - злоумышленник может получить полные права для доступа к целевому компьютеру. Поэтому способ шифрования и способ передачи данных для авторизации между компонентами не документируется. К тому же пароль передаётся не в чистом виде, а в виде хеша, который сравнивается с хешем реального пароля.

4.winlogon

Winlogon - этот процесс управляет входом пользователей в систему и выходом из нее.

Функции

Процесс Winlogon начинает работу, будучи запущенным процессом SMSS. После некоторых подготовительных действий, Winlogon отображает приглашение к входу в систему Windows. В ходе запуска ОС Winlogon запускает LSASS и Services.exe. Если активен новый стиль экрана приветствия, то для его отображения запускается процесс «logonui.exe». После входа в систему Winlogon запускает программы, прописанные в параметре Userinit - обычно «userinit.exe». Эта программа выполняет запуск программ, прописанных в параметре Shell - обычно «explorer.exe».

5.csrss.exe

Это часть подсистемы Win32, исполняющаяся в пользовательском режиме (в то время как Win32.sys исполняется в режиме ядра). Csrss означает *client/server run-time subsystem* (подсистема клиент/сервер времени исполнения) и представляет собой существенную подсистему, которая должна быть запущена всегда. Подсистема csrss отвечает за работу консольных окон, создание и уничтожение потоков и частично за работу 16-разрядной виртуальной среды MS-DOS.

По умолчанию его завершение в Диспетчере задач запрещено. Завершение csrss.exe каким-либо другим способом ведёт к аварийной перезагрузке Windows.

6.smss.exe

SMSS.EXE - данный процесс представляет подсистему менеджера сеансов.

Данная подсистема является ответственной за запуск пользовательского сеанса. Этот процесс инициализируется системным потоком и ответствен за различные действия, включая запуск процессов Winlogon и Win32 (Csrss.exe) и установку системных переменных. После запуска данных процессов процесс Smss ожидает их завершения. При «нормальном» завершении процессов система корректно завершает работу. Если процессы завершаются аварийно, процесс Smss.exe заставляет систему прекратить отвечать на запросы. Этот процесс нельзя завершить из менеджера задач.

Процесс SMSS отвечает за:

- инициализацию переменных окружения;
- запуск процессов CSRSS и Winlogon;
- контроль работы процесса Winlogon;
- запуск программы CHKDSK (Autochk) и других программ, запускаемых из раздела реестра Boot Execute;
- выполнение «Pending rename operations» - операций по удалению, перемещению или копированию файлов до полной загрузки;
- загрузку Known DLL - библиотек для работы windows-приложений (advapi32.dll, user32.dll, kernel32.dll и др.). Если хотя бы одна из этих библиотек не будет загружена, произойдёт экстренная перезагрузка или крах системы.

SVCHOST.EXE

(Generic Host Process for Win32 Services)

Очень часто у пользователей возникает вопрос - что это за приложение «svchost.exe», наблюдаемое ими в списке процессов, и почему оно загружено в нескольких экземплярах?

SVCHOST.EXE - это главный системный процесс для тех служб, которые запускаются из динамически загружаемых библиотек (DLL-файлов).

Действительно несколько экземпляров процесса svchost.exe могут быть запущены одновременно. Так как каждый из таких экземпляров представляет собой определенную преимущественно системную службу или же группу служб. Эти группы определены в следующем разделе реестра:

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SvcHost

Каждый параметр этого раздела представляет собой отдельную Svchost-группу и отображается при просмотре активных процессов, как отдельный экземпляр svchost.exe.

Также, чтобы просмотреть список служб, выполняющихся в каком-либо процессе svchost.exe, можно сделать следующее:

Start > Run (Пуск > Выполнить)

Вписываем: CMD

Нажимаем ОК или клавишу ENTER.

В появившемся приложении вводим команду: tasklist /SVC

И нажимаем на клавишу ENTER.

```
Image Name                     PID Services
========================= ====== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       708 N/A
csrss.exe                      756 N/A
winlogon.exe                   780 N/A
services.exe                   824 Eventlog, PlugPlay
lsass.exe                      836 PolicyAgent, ProtectedStorage, SamSs
svchost.exe                    984 DcomLaunch, TermService
svchost.exe                   1044 RpcSs
svchost.exe                   1084 AudioSrv, CryptSvc, Dhcp, dmserver,
                                   EventSystem, lanmanserver,
                                   lanmanworkstation, Netman, Nla, RasMan,
                                   Schedule, seclogon, SENS, SharedAccess,
                                   ShellHWDetection, srservice, TapiSrv,
                                   Themes, TrkWks, W32Time, winmgmt, wuauserv,
                                   WZCSVC
svchost.exe                   1180 Dnscache
svchost.exe                   1216 LmHosts, SSDPSRV, WebClient
```

Список служб Windows XP, запускаемых с помощью svchost.exe:

(т.е. эти службы не являются вирусами!)

Английское название	Русское название
Alerter	Оповещатель
Application Management	Управление приложениями
Automatic Updates	Автоматическое обновление
Background Intelligent Transfer Service	Фоновая интеллектуальная служба передачи
COM+ Event System	Система событий COM+
Computer Browser	Обозреватель компьютеров
Cryptographic Services	Службы криптографии
DHCP Client	DHCP-клиент
Distributed Link Tracking Client	Клиент отслеживания изменившихся связей
DNS Client	DNS-клиент

Error Reporting Service	Служба регистрации ошибок
Fast User Switching Compatibility	Совместимость быстрого переключения пользователей
Help and Support	Справка и поддержка
Human Interface Device Access	Доступ к HID-устройствам
Logical Disk Manager	Диспетчер логических дисков
Messenger	Служба сообщений
Network Connections	Сетевые подключения
Network Location Awareness (NLA)	Служба сетевого расположения (NLA)
Portable Media Serial Number Service	Серийный номер переносного медиа-устройства
Remote Access Auto Connection Manager	Диспетчер авто-подключений удаленного доступа
Remote Access Connection Manager	Диспетчер подключений удаленного доступа
Remote Procedure Call (RPC)	Удаленный вызов процедур (RPC)
Remote Registry	Удаленный реестр
Removable Storage	Съемные ЗУ
Routing and Remote Access	Маршрутизация и удаленный доступ
Secondary Logon	Вторичный вход в систему
Security Center	Центр обеспечения безопасности
Server	Сервер
Shell Hardware Detection	Определение оборудования оболочки
SSDP Discovery Service	Служба обнаружения SSDP
System Event Notification	Уведомление о системных событиях
System Restore Service	Служба восстановления системы
Task Scheduler	Планировщик заданий
TCP/IP NetBIOS Helper	Модуль поддержки NetBIOS через TCP/IP
Telephony	Телефония
Terminal Services	Службы терминалов
Themes	Темы
Universal Plug and Play Device Host	Узел универсальных PnP-устройств
Upload Manager	Диспетчер отгрузки
WebClient	Веб-клиент
Windows Audio	Windows Audio
Windows Firewall/Internet Connection Sharing (ICS)	Брандмауэр Интернета (ICF)/Общий доступ к Интернету (ICS)
Windows Image Acquisition (WIA)	Служба загрузки изображений (WIA)
Windows Management Instrumentation	Инструментарий управления Windows
Windows Management Instrumentation Driver Extensions	Расширения драйверов WMI
Windows Time	Служба времени Windows
Wireless Zero Configuration	Беспроводная настройка

Workstation	Рабочая станция

Список «левых» служб, ссылающихся на svchost.exe:

(т.е. эти службы были созданы вирусами!)

Название службы	Командная строка
AppMgmt	svchost.exe -k AppMgmt
Browser	svchost.exe -k Browser
COM Message Transfer (mscommt)	svchost.exe -k mscommt
Disk Monitor Services (DiskMon32)	svchost.exe -k dmon
dmserver	svchost.exe -k
DNS Server (DNS Server)	svchost.exe
FastUserSwitchingCompatibil (Fast User Switching Compatibil)	svchost.exe
Generic Host Process For Win32 Services (Generic Host Process)	svchost.exe
generic host process (svchost)	svchost.exe
Hardware Detection (Serv-U)	svchost.exe
Host Services (Host Services)	svhosts.exe
IPRIP (IPRIP)	svchost.exe -k netsvcs
kdc	svchost.exe -k kdc
LmHosts	svchost.exe -k LmHosts
Messenger	svchost.exe -k Messenger
MS Internet Countermeasures Framework (ICF)	\System32:svchost.exe
NetLogon	svchost.exe -k
Network Connections Sharing (RpcTftpd)	svchost.exe
Network DDE DSMA (NetDDEdsma)	svchost.exe
ntmssvc	svchost.exe -k ntmssvc
NVIDIA Driver ServiceЎЎ (NVSv)	svchost.exe
RasAt (Remote Connection)	svchost.exe
Policy Agent	svchost.exe -k Policy Agent
Power Manager (PowerManager)	svchost.exe
ProtectedStorage	svchost.exe -k ProtectedStorage
Server Management Service	svchost.exe
SVC Module (SVC Module)	svchost.exe
svchost	SVCHOST.EXE
svchost.exe (moto)	svchost.exe
svchost.exe (moto)	любое название из 18-ти знаков
svchost.exe (svchost.exe)	svchost.exe
System Event Messaging	svchost.exe
taskmng (svchost)	svchost.exe
TrkSvr	svchost.exe -k TrkSvr
TrkWks	svchost.exe -k TrkWks

W32Time	svchost.exe -k W32Time
Windows Configuration Backup Service (CfgBackupSvc)	svchost.exe
Windows Configuration Loader (Windows Configuration Loader)	SVCHOST.EXE
Windows Configuration Manager (ConfigMgr)	svchost.exe
Windows Kernel (Windows Kernel)	svchost.exe
Windows Management (Windows Management)	svchost.exe
Windows Network Mapping Service (NetMap)	svchost.exe
Windows Security Drivers (csrs)	svchost.exe
Windows Smrss Service	svchost.exe
.NET Framework Service	svchost.exe
.NET Framework Service (.NET Connection Service)	svchost.exe

Обязательно нужно иметь в виду, что системный файл svchost.exe должен находиться в папке:

C:\WINDOWS\system32 (касается только Windows XP/NT/2000)

Если он находится в папке WINDOWS и/или файлов с таким названием в вашей системе несколько, то, скорее всего, у вас живет вирус, так как несколько копий файла svchost.exe - это всё-таки еще не гарантия заражения.

Например, вас ни в коем случае не должны пугать копии файла svchost.exe в таких папках, как:

C:\WINDOWS\ServicePackFiles\i386

C:\WINDOWS\Prefetch.

Или, к примеру, файл с названием svchost.exe создается при установке антивируса BullGuard:

C:\Program Files\BullGuard Software\svchost.exe, который также к вирусам никакого отношения не имеет.

Поэтому, в первую очередь, обращать внимание нужно именно на папку WINDOWS, т.к. она наиболее часто используется в целях маскировки под настоящий файл svchost.exe.

Наиболее распространенные местоположения вирусов, маскирующихся под svchost.exe:

C:**WINDOWS**\svchost.exe

C:\WINDOWS**system**\svchost.exe (касается только Windows XP/NT/2000)

C:\WINDOWS**config**\svchost.exe

C:\WINDOWS**inet20000**\svchost.exe

C:\WINDOWS**inetsponsor**\svchost.exe

Помимо этого очень многие вирусы пытаются себя замаскировать, используя имена и названия, которые очень похожи на название «svchost» (в этом случае местоположение файлов уже может быть абсолютно любое, в том числе достаточно часто используется и папка WINDOWS\system32).

Также обязательно должно насторожить, если svchost.exe (или что-либо похожее) каким-либо образом пытается записать себя в обычную

автозагрузку (т.е. помимо запуска в качестве системной службы, использует Windows StartUp или ini-файлы).

Провести работу с программами: avz4, Windowviewer, ProcessExplorer, Autoruns, ProcessKiller, Security Task Manager и обнаружить все скрытые процессы.

Итоговый контрольный тест.

К сервисам безопасности относят:

- ☐ идентификация/аутентификация;
- ☐ протоколирование/аудит;
- ☐ шифрование;
- ☐ аудит.

2. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:

- ☐ прослушивание каналов;
- ☐ умышленное уничтожение или искажение информации;
- ☐ выход из строя операционной системы;
- ☐ внедрение сетевых вирусов.

3. Конфиденциальность - это:

- ○ предотвращение пассивных атак для передаваемых или хранимых данных;
- ○ защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных;
- ○ подтверждении подлинности взаимодействующих объектов;
- ○ защита от несанкционированного использования ресурсов сети.

4. К механизмам безопасности относят:

- ☑ хэш-функции;
- ☐ целостность сообщения;
- ☐ алгоритмы симметричного шифрования;
- ☐ невозможность отказа от полученного сообщения.

5. Активные угрозы становятся видимыми на уровне (модели OSI):

- ○ физическом;
- ○ канальном;
- ○ сетевом;
- ○ транспортном.

6. Алгоритм, использующий для шифровки два разных ключа (открытый и закрытый):

- ○ алгоритм симметричного шифрования;
- ○ алгоритм асимметричного шифрования;
- ○ алгоритм использования контрольных сумм;
- ○ алгоритм проверки подлинности.

7. Двоичные программы, внедряемые в web-страницу:

- [ ] JavaScript;
- [ ] Java-апплеты;
- [ ] activeX;
- [ ] VBScript.

8. Цифровая подпись – это:

- способ введения электронной метки для файла данных;
- файл, подтверждающий ваши права;
- сведения о пользователе помещаемые в файл;
- идентификатор документа.

9. Обозначение, семейства протоколов охватывающих проблемы безопасности на IP-уровне:

- FTP;
- UDP;
- TCP/IP;
- Ipsec.

10. Основные протоколы транспортного уровня, применяемые в Интернете:

- [ ] FTP;
- [ ] STP;
- [ ] TCP;
- [ ] UDP.

11. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:

- [ ] прослушивание каналов;
- [ ] умышленное уничтожение или искажение информации;
- [ ] выход из строя операционной системы;
- [ ] внедрение сетевых вирусов.

12. _____каналов – это запись и последующий анализ всего проходящего потока сообщений.

13. К сервисам безопасности относят:

- идентификация/аутентификация;
- протоколирование/аудит;
- шифрование;
- аудит.

14. _____ – это предотвращение пассивных атак для передаваемых или хранимых данных.

15. _____- подтверждении подлинности взаимодействующих объектов.

16. Контроль _____ – защита от несанкционированного использования ресурсов.

17. Соответствие между понятиями и их определениями:

1	Конфиденциальность	это предотвращение пассивных атак для передаваемых или хранимых данных
2	Аутентификация	защита от несанкционированного использования ресурсов
3	Контроль доступа	подтверждении подлинности взаимодействующих объектов

18. Цифровая подпись – это:

- способ введения электронной метки для файла данных;
- файл, подтверждающий ваши права;
- сведения о пользователе помещаемые в файл;
- идентификатор документа.

19. К механизмам безопасности относят:

- хэш-функции;
- целостность сообщения;
- алгоритмы симметричного шифрования;
- невозможность отказа от полученного сообщения.

20. Активные угрозы становятся видимыми на уровне (модели OSI):

- физическом;
- канальном;
- сетевом;
- транспортном.

21. Комплекс мероприятий, направленных на обеспечение информационной безопасности:

- защита информации;
- информационная защита;
- безопасность информации;
- информационная безопасность.

22. Преимущества использования стандартных правил, регламентирующих работу пользователей:

- рутинные задачи всегда выполняются одинаково;
- уменьшение вероятности появления ошибок;
- работа по инструкциям выполняется гораздо быстрее;
- все выше перечисленное.

23. Совокупность всех объектов, атрибутов объектов и правил (синтаксиса атрибутов) в Active Directory

24. Политика безопасности сети на основе Windows храниться в следующих типах объектов:

- локальный объект групповой политики;
- глобальный объект групповой политики;

- ☐ объект групповой политики домена.

25. Параметры узла *Конфигурация компьютера* в редакторе объектов групповой политики определяют работу:

- ○ пользователя;
- ○ компьютера;
- ○ операционной системы;
- ○ все выше перечисленное.

26. Компонент групповой политики, определяющая параметры реестра, задающий внешний вид рабочего стола и компоненты операционной системы:

- ○ административные шаблоны;
- ○ параметры безопасности;
- ○ установка программ;
- ○ сценарии.

27. Программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента:

- ○ сервер;
- ○ клиент;
- ○ компьютер;
- ○ пользователь.

28. Сервер, в основную задачу которого входит предоставление доступа к файлам на диске:

- ○ файл-сервер;
- ○ контроллер домена;
- ○ терминальный сервер.

29. Операции, выполняемые посредством оснастки Пользователи и компьютеры:

- ○ создание пользователей;
- ○ создание групп;
- ○ создание контейнеров;
- ○ все выше перечисленное.

30. Основной компонент IIS:

- ○ веб-сервер;
- ○ ftp-сервер;
- ○ почтовый сервер.

3.2. Оценочные средства промежуточной аттестации

Перечень теоретических вопросов для зачета:

1. Информация как объект защиты. Цели защиты информации.
2. Информационная безопасность. Понятие. Аспекты. Угрозы информационной безопасности.

3. Меры по формированию режима информационной безопасности. Принципы системы защиты.

4. Аппаратно-программные средства защиты информации. Системы шифрования дисковых данных и данных, передаваемых по сетям.

5. Аппаратно-программные средства защиты информации. Системы аутентификации электронных данных и средствах управления криптографическими ключами.

6. Причины взлома систем защит информации и способы заинтересовать пользователя в лицензионном ПО.

7. Анализ опыта защиты информации в АСОД.

8. Общий анализ проблемы защиты информации в современных АСОД.

9. Виды криптографического закрытия информации. Подробно два способа шифрования.

10. Электронная подпись в системах с открытым ключом.

11. Способы привязки к компьютеру.

12. Функции систем защиты информации от несанкционированного доступа.

13. Идентификация и аутентификация пользователя. Определения. Формы хранения данных о пользователе. Структура данных о пользователе.

14. Две типовые схемы идентификации и аутентификации.

15. Взаимная проверка подлинности пользователей.

16. Компьютерные вирусы. Классификация вирусов по способу заражения среды обитания.

17. Компьютерные вирусы. Классификация вирусов по деструктивным действиям.

18. Защита от вирусов. Организационно-технические меры. Общие способы защиты. Средства, учитывающие специфику работы фрагментов системы.

19. Компьютерные атаки. Определение. Модели.

20. Этапы реализации компьютерной атаки. Сбор информации.

21. Этапы реализации компьютерной атаки. Реализация и завершение.

22. Классификация компьютерных атак.

23. Основные задачи и дополнительные функции средств обнаружения компьютерных атак.

Перечень типовых задач (для оценки умений):

1. Криптография: зашифровать алгоритмом RSA сообщение.
2. Криптография: расшифровать сообщение.
3. Криптография: подписать документ электронной цифровой подписью.
4. Описать основные системные процессыWindows.
5. Просмотреть траффик сети.
6. Просканировать компьютер на наличие вредоносного ПО.
7. Проверить компьютер на наличие вирусов.
8. Настроить удаленный доступ к компьютеру.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1. Описание процедур проведения текущего контроля успеваемости студентов

В таблице представлено описание процедур проведения контрольно-оценочных мероприятий текущего контроля успеваемости студентов, в соответствии с рабочей программой дисциплины, и процедур оценивания результатов обучения с помощью запланированных оценочных средств.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Реферат	Задание по написанию реферата выдается в начале каждого модуля. Работа выполняется во внеучебное время и должна быть сдана в назначенный срок. Критерии оценки реферата озвучиваются на первой вводной лекции по предмету.
Доклад	Темы докладов озвучиваются в начале изучения каждого модуля, также объявляются критерии оценки доклада. Студенты делают доклад во время лекционного занятия по рассматриваемой теме.
Лабораторная работа	Практическая работа выполняется каждым студентом индивидуально во время практических занятий. Для выполнения каждой практической работы выделяется определенное время, в зависимости от объема работы 1 или 2 пары, после этого времени отчет по практической работе должен быть сдан преподавателю на проверку. Критерии оценки практических работ озвучиваются на первой вводной лекции по предмету.
Конспект	Задание по составлению конспекта выдается в начале каждого модуля. Работа выполняется во внеучебное время и должна быть сдана в назначенный срок. Критерии оценки конспекта озвучиваются на первой вводной лекции по предмету.
Итоговый контрольный тест	О проведении итогового тестирования объявляется студентам не менее чем за неделю. Итоговое контрольное тестирование проводится в учебное время, на выполнение работы отводится одна пара. Критерии оценки и требования к выполнению итогового контрольного теста озвучиваются студентам не менее чем за неделю. В конце отведенного для выполнения времени, выполненные работы сдаются на проверку.

Методика оценки деятельности студента

Модуль	Номер раздела	Процедура оценивания*	Оценка	
			min	*max*
1		Лабораторная работа Конспект Реферат Доклад	4 2 3 3	8 4 5 5
2		Лабораторная работа Конспект Реферат Доклад	4 2 3 3	8 4 5 5

3		Лабораторная работа Конспект Реферат Доклад	4 2 3 3	8 4 5 5
4		Лабораторная работа Конспект Реферат Доклад Итоговый контрольный тест	4 2 3 3 7	8 4 5 5 12
всего			55	100

4.2. Описание процедур проведения промежуточной аттестации

Зачет

При определении уровня достижений обучающих на зачете учитывается:

- знание программного материла и структуры дисциплины;
- знания, необходимые для решения типовых задач, умение выполнять предусмотренные программой задания;
- владение методологией дисциплины, умение применять теоретические знания при решении задач, обосновывать свои действия.