ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
БИРСКИЙ ФИЛИАЛ УУНиТ
ФАКУЛЬТЕТ ФИЗИКИ И МАТЕМАТИКИ

Утверждено:
на заседании кафедры информатики и экономики
протокол № 4 от 24.11.2022 г.
Зав. кафедрой *подписано ЭЦП* /Мухаметшина Г.С.

Согласовано:
Председатель УМК
факультета физики и математики
подписано ЭЦП /Бигаева Л.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
для очной формы обучения

Методы и средства защиты информации и образовательной среды
Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки (специальность)
44.03.05 *Педагогическое образование (с двумя профилями подготовки)*

Направленность (профиль) подготовки
Математика, Информатика

Квалификация
Бакалавр

Разработчик (составитель) Старший преподаватель (должность, ученая степень, ученое звание)	*подписано ЭЦП* /Красильников В.А. (подпись, Фамилия И.О.)

Для приема: 2023 г.

Бирск 2022 г.

Составитель / составители: Красильников В.А. ____________________

Рабочая программа дисциплины утверждена на заседании кафедры информатики и экономики протокол № ___ от «___» _________ 20__ г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	Способен использовать базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам (ПК-2);	ПК-2.1. Знать предметную область профильных дисциплин	Знает базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам
		ПК-2.2. Уметь анализировать предметную область профильных дисциплин	Умеет использовать базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам
		ПК-2.3. Владеть опытом и навыками использования знаний и умений и навыков в предметной области для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Владеет навыками использования базовых научно-теоретических знаний, практических умений, методов и средств защиты информации для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам
	Способен организовывать	ПК-3.1. Знать основы проектно-	Знает, как организовывать

	проектно-исследовательскую деятельность обучающихся для достижения результатов обучения (ПК-3);	исследовательской деятельности обучающихся	проектно-исследовательскую деятельность обучающихся для достижения результатов обучения
		ПК-3.2. Уметь планировать, реализовывать, контролировать проектно-исследовательскую деятельность обучающихся	Умеет организовывать проектно-исследовательскую деятельность обучающихся для достижения результатов обучения
		ПК-3.3. Владеть опытом и навыками организации проектно-исследовательской деятельности обучающихся	Владеет навыками организации проектно-исследовательской деятельности обучающихся для достижения результатов обучения

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства защиты информации и образовательной среды» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе в 10 семестре.

Цель изучения дисциплины: формирование знаний о видах угроз информационной безопасности и её стандартах, методах и средствах борьбы с угрозами информационной безопасности, представлений о политике безопасности и её типах, умений и навыков решать задачи, связанные с обеспечением информационной безопасности при проектировании, внедрении и эксплуатации информационных систем, способность использовать основы правовых знаний в различных сферах деятельности.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
БИРСКИЙ ФИЛИАЛ УУНиТ
ФАКУЛЬТЕТ ФИЗИКИ И МАТЕМАТИКИ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «Методы и средства защиты информации и образовательной среды» на 10 семестр

очная

форма обучения

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	2/72
Учебных часов на контактную работу с преподавателем:	48.2
лекций	16
практических/ семинарских	16
лабораторных	16
контроль самостоятельной работы (КСР)	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	0.2
Учебных часов на самостоятельную работу обучающихся (СРС)	23.8
Учебных часов на подготовку к зачету (Контроль)	0

Форма контроля:
Зачет 10 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		Лек	Лаб	П	Зч	СРС			
5 курс / 10 семестр									
1	Раздел 1. Информационные ресурсы. Информационная безопасность								
1.1	Информационные ресурсы Основные понятия, классификация информационных ресурсов	2	2	4		4	Осн. лит-ра №№ 1,2 Доп. лит-ра № 2	Конспект	Лабораторная работа, Практические работы, Тестирование, Групповой опрос
1.2	Информационная безопасность Понятие информационной безопасности, классификация.Основные составляющие информационной безопасности. Классификация методов обеспечения информационной безопасности	4	2	4		4	Осн. лит-ра №№ 1,2 Доп. лит-ра №№ 1,2	Конспект	Групповой опрос, Тестирование, Лабораторная работа, Практические работы
2	Раздел 2. Методы и средства защиты информации. Компьютерная безопасность.								

2.1	Методы и средства защиты информации. Правовая защита. Организационная защита. Инженерно-техническая защита. Криптографические средства защиты	6	4	4		7.8	Осн. лит-ра №№ 1,2 Доп. лит-ра № 2	Конспект	Тестирование, Групповой опрос, Практические работы, Лабораторная работа
2.2	Компьютерная безопасность. Защита компьютерной информации от несанкционированного доступа. Угрозы безопасности информации в компьютерных системах. Парольная защита операционных систем	4	8	4		8	Осн. лит-ра №№ 1,2 Доп. лит-ра №№ 1,2	Конспект	Практические работы, Лабораторная работа, Тестирование, Групповой опрос
3	Зачет				1	0.2			
Итого по 5 курсу 10 семестру		16	16	16	1	24			
Итого по дисциплине		16	16	16	1	24			

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

Код и формулировка компетенции: Способен использовать базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам (ПК-2);

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (Зачет)	
		Незачтено	Зачтено
ПК-2.1. Знать предметную область профильных дисциплин	Знает базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Знания не сформированы	Знания полностью сформированы
ПК-2.2. Уметь анализировать предметную область профильных дисциплин	Умеет использовать базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Умения не сформированы	Умения в основном сформированы

ПК-2.3. Владеть опытом и навыками использования знаний и умений и навыков в предметной области для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Владеет навыками использования базовых научно-теоретических знаний, практических умений, методов и средств защиты информации для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Владение навыками не сформировано	Владение навыками в основном сформировано

Код и формулировка компетенции: Способен организовывать проектно-исследовательскую деятельность обучающихся для достижения результатов обучения (ПК-3);

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (Зачет)	
		Незачтено	Зачтено
ПК-3.1. Знать основы проектно-исследовательской деятельности обучающихся	Знает, как организовывать проектно-исследовательскую деятельность обучающихся для достижения результатов обучения	Знания не сформированы	Знания полностью сформированы
ПК-3.2. Уметь планировать, реализовывать, контролировать проектно-исследовательскую деятельность	Умеет организовывать проектно-исследовательскую деятельность обучающихся для	Умения не сформированы	Умения в основном сформированы

обучающихся	достижения результатов обучения		
ПК-3.3. Владеть опытом и навыками организации проектно-исследовательской деятельности обучающихся	Владеет навыками организации проектно-исследовательской деятельности обучающихся для достижения результатов обучения	Владение навыками не сформировано	Владение навыками в основном сформировано

Критериями оценивания являются баллы, которые выставляются за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины. Баллы, выставляемые за конкретные виды деятельности представлены ниже.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-2.1. Знать предметную область профильных дисциплин	Знает базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Групповой опрос, Конспект, Тестирование, Лабораторная работа, Практические работы
ПК-2.2. Уметь анализировать предметную область профильных дисциплин	Умеет использовать базовые научно-теоретические знания, практические умения и навыки по предмету для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	Практические работы, Групповой опрос, Конспект, Тестирование, Лабораторная работа
ПК-2.3. Владеть опытом и навыками использования знаний и умений и навыков в	Владеет навыками использования базовых научно-теоретических знаний,	Лабораторная работа, Практические работы

предметной области для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	практических умений, методов и средств защиты информации для проектирования и реализации образовательного процесса по дополнительным общеобразовательным программам	
ПК-3.1. Знать основы проектно-исследовательской деятельности обучающихся	Знает, как организовывать проектно-исследовательскую деятельность обучающихся для достижения результатов обучения	Конспект, Тестирование, Лабораторная работа, Практические работы, Групповой опрос
ПК-3.2. Уметь планировать, реализовывать, контролировать проектно-исследовательскую деятельность обучающихся	Умеет организовывать проектно-исследовательскую деятельность обучающихся для достижения результатов обучения	Тестирование, Лабораторная работа, Практические работы, Групповой опрос, Конспект
ПК-3.3. Владеть опытом и навыками организации проектно-исследовательской деятельности обучающихся	Владеет навыками организации проектно-исследовательской деятельности обучающихся для достижения результатов обучения	Лабораторная работа, Практические работы

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины

для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов.

Тестовые задания

Описание тестовых заданий: тестовые задания включают тесты закрытого типа (с одним правильным ответом), тесты на установлении последовательности и на установление соответствия. Оценка за выполнение тестовых заданий выставляется на основании процента заданий, выполненных студентами в процессе прохождения промежуточного и рубежного контроля знаний

Какой из перечисленных способов подключения к сети Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам:

1.терминальное соединение по коммутируемому телефонному каналу;

2.временный доступ по телефонным каналам;

3.постоянное соединение по оптоволоконному каналу;

4.постоянное соединение по выделенному каналу;

5.удаленный доступ по телефонным каналам?

Компьютер, подключенный к сети Internet, обязательно имеет

1.WEB-страницу;
2.URL-адрес;
3.доменное имя;
4.IP-адрес;
5.домашнюю WEB-страницу

Комплекс аппаратных и программных средств, позволяющих компьютерам обмениваться данными, - это:
1.магистраль;
2.адаптер;
3.интерфейс;
4.шины данных;
5.компьютерная сеть.
Формы защиты интеллектуальной собственности -
: авторское, патентное право и коммерческая тайна
: интеллектуальное право и смежные права
: коммерческая и государственная тайна
: гражданское и административное право

По принадлежности информационные ресурсы подразделяются на
: государственные, коммерческие и личные
: государственные, не государственные и информацию о гражданах
: информацию юридических и физических лиц
: официальные, гражданские и коммерческие

К негосударственным относятся информационные ресурсы
: созданные, приобретенные за счет негосударственных учреждений и организаций
: созданные, приобретенные за счет негосударственных предприятий и физических лиц
: полученные в результате дарения юридическими или физическими лицами
: все указанные

Методические материалы, определяющие процедуру оценивания выполнения тестовых заданий

Описание методики оценивания выполнения тестовых заданий: оценка за выполнение тестовых заданий ставится на основании подсчета процента правильно выполненных тестовых заданий.
Критерии оценки (в баллах)*:*
- **9-10** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 81 – 100 %;
- **7-8** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 61 – 80 %;
- **4-6** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 41 – 60 %;
- **до 4** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 40 %;

Конспект

Темы для конспектов:
Достоинства и недостатки реализации и обработки радиотехнических сигналов цифровыми методами.
Кодирование информации
«Несанкционированный» и «неавторизованный «доступ к информации».
Разница между “защитой информации” и “информационной безопасностью”
Блокировка неавторизованного доступа к информации.

Методические материалы, определяющие процедуру оценивания конспекта

Критерии оценки:
- оптимальный объем текста (не более одной трети оригинала);
- логическое построение и связность текста;
- полнота/ глубина изложения материала (наличие ключевых положений, мыслей);
- визуализация информации как результат ее обработки (таблицы, схемы, рисунки);
- оформление (аккуратность, соблюдение структуры оригинала).

1- выставляется, если текст конспекта оформлен аккуратно, выбрано главное и второстепенное, выделены ключевые слова и понятия, конспект написан лаконично с применением системы условных сокращений.

Практические работы

Практические работы, являются важным источником познания нового материала, способствуют формированию и совершенствованию практических умений и навыков обучающихся.
Практические работы
Практическая работа № 2

«ЦИФРОВАЯ ПОДПИСЬ»

Цель работы – Освоение практических навыков применения цифровой подписи. Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

- материал

Цифровая подпись

PGP (Pretty Good Privacy) - программа, служащая для кодирования и/или подписывания сообщений, файлов и любой другой информации, представленной в электронном виде. В основе работы PGP лежит алгоритм RSA (Rivest-Shamir-Adelman), основанный на наличии двух ключей - открытого и секретного. Открытый ключ распространяется максимальному кол-ву людей (через KeyServer'a, лично, и т.п.), а секретный должен находиться только у владельца (причем в надежном месте, если к компьютеру на котором Вы работаете, имеют доступ другие люди - храните свой секретный ключ на дискете).

Криптостойкость алгоритма RSA основывается на том, что современной математике не известны алгоритмы разложения больших простых (рекомендую использовать ключи не менее 1024 бит) чисел за реальное время.

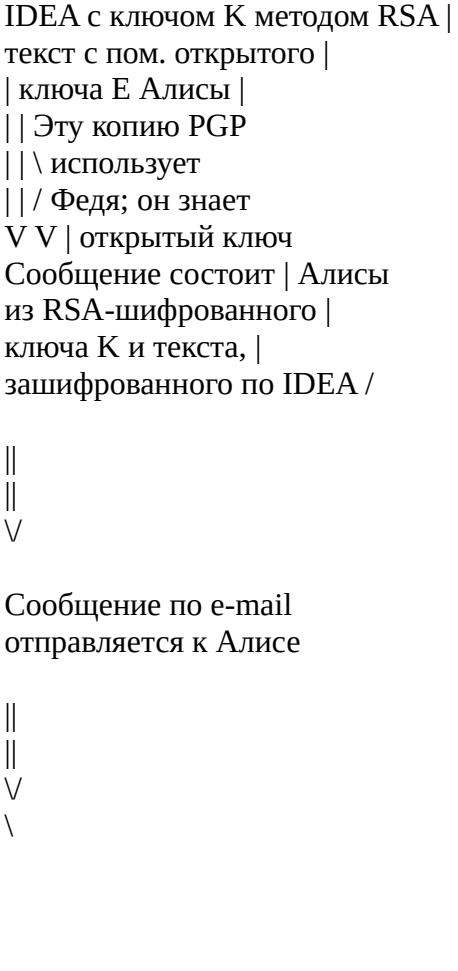
Итак, Вы хотите передать мне какой-либо файл по электронной почте и при этом быть уверенным, что никто другой кроме меня не сможет прочитать этот файл - Вы берете мой открытый ключ, кодируете им свой файл и отправляете файл мне. Никто кроме меня (включая Вас) не сможет прочитать этот закодированный файл без моего секретного ключа. Другой пример - Вы хотите, отправляя свои письма быть уверенным в том, что никто не исказил содержимого письма, для этого Вы подписываете письмо электронной подписью с помощью Вашего секретного ключа и посылаете его (письмо). Получив Ваше письмо и обладая Вашим открытым ключом, я могу удостовериться в том, что ни один бит информации не был искажен при прохождении письма.

Для начала нужно создать пару ключей (открытый и закрытый). Это делается с помощью программы PGPkeys. Рекомендуется использовать ключи не менее 1024 бит. Ваша пара ключей занесется в общий список доступных Вам ключей (в основном конечно открытых). Теперь имея пару ключей Вы можете легко подписывать, кодировать файлы

Рекомендуется делать резервную копию базы данных открытых ключей (pubring.pkr), а также хранить секретный ключ (secring.skr) и файл randseed.bin на дискете доступной только Вам.

Описание основ PGP

PGP представляет собой гибридную систему, которая включает в себя алгоритм с открытым ключом (асимметричный алгоритм) и обычный алгортм с секретным ключом (симметричный алгоритм), что дает высокую скорость, характерную для симметричных алгоритмов и существенные удобства, характерные для криптографии с открытым ключом. С точки зрения пользователя PGP ведет себя как система с открытым ключом. В криптосистемах с открытым ключом генерируется с помощью специального математического алгоритма пара ключей - один открытый и один секретный. Сообщение шифруется с помощью одного ключа, и дешифруется с помощью другого (причем неважно каким именно из двух ключей производится шифрование). Сообщение *нельзя* расшифровать с помощью ключа шифрования. Обычно вы опубликовываете свой открытый ключ, делая его доступным любому, кто захочет послать вам зашифрованное сообщение. Такой человек зашифрует сообщение вашим открытым ключом, при этом ни он сам, ни кто другой не могут расшифровать шифрованное сообщение. Только вы можете расшифровать сообщение, то есть тот человек, который имеет секретный ключ, соответствующий открытому ключу. Очевидно, что секретный ключ должен храниться в секрете своим обладателем.
Огромным преимуществом такого способа шифровки является то, что в отличие от обычных методов шифрования, нет необходимости искать безопасный способ передачи ключа адресату. Другой полезной чертой таких криптосистем является возможность создать цифровую "подпись" сообщения, зашифровав его своим секретным ключом. Теперь, с помощью вашего открытого ключа любой сможет расшифровать сообщение и таким образом убедиться, что его зашифровал действительно владелец секретного ключа.
PGP использует для шифрования алгоритм с открытым ключом RSA в паре с обычным методом шифрования IDEA. В методе IDEA для шифрования используется один ключ, и как и в других симметричных криптосистемах, тот же ключ дешифровывает сообщение. PGP использует алгоритм RSA для зашифровки ключа IDEA с помощью открытого ключа адресата. Адресат, приняв сообщение с помощью PGP, расшифрует этот секретный ключ IDEA. Далее остальная часть сообщения расшифровывается принимающей стороной методом IDEA.



Ключ IDEA расшифровывается |
секретным ключом RSA Алисы | Алиса
| использует
|| \ свою копию PGP
|| / и знает свой
\/ | секретный
| ключ.
Текст расшифровывается |
с пом. ключа IDEA /

Математические основы RSA

RSA использует операцию возведения в степень по модулю для шифровки и дешифровки сообщения, которое получается путем перевода текста в цифровую форму.

Алгоритм RSA и генерация ключей

Функция шифровки, используемая в RSA, выглядит так *C = T^E mod N*, где *T* представляет собой шифруемый текст, *C* - зашифрованный текст, а *E* представляет собой открытый ключ. Другими словами, *T* возводится в степень *E* по модулю *N*. Для примера, 2 в степени 3 дает 8, а 2 в степени 3 по модулю 7 есть 8 mod 7, что равно 1. Функция дешифрования выглядит так: *T = C^D mod N* где *D* представляет собой секретный ключ. Пара ключей *E* и *D* должна быть выбрана так, что *E* является обратным к *D* по отношению к операции возведения в степень по модулю *N*. Иными словами, *(T^E mod N)^D mod N = T^ED mod N = T*.

Для того, чтобы найти подходящую пару, для которой это равенство верно, нам надо знать *функцию Эйлера переноса? (Euler's totient function), J(N)* для данного значения модуля *N*. Функция Эйлера представляет собой количество чисел в интервале от 1 до *N-1*, которые являются *простыми относительно N*. Для нахождения функции *J(N)* недо, в свою очередь, найти простые факторы *N*.

Фундаментальная теорема арифметики: Любое не простое число может быть представлено как произведение уникального набора простых чисел.

Относительно простые числа: Два числа называются относительно простыми, если среди их простых факторов нет одинаковых.

Итак, нам надо найти набор простых факторов числа *N* для того, чтобы вычислить функцию Эйлера. *J(N)*. Нахождение этих факторов является задачей *чрезвычайно* сложной - практически абсолютно невозможно для достаточно больших *N*, и именно этот факт и делает PGP таким надежным методом шифрования. Для заданных *N* и *E* вы не можете найти *D* (и, таким образом, расшифровать сообщение) не зная простых факторов числа *N*, что настолько трудно, что PGP является виртуально невскрываемой при достаточно больших *N*.

Практический способ сгенерировать пару ключей - это сначала сгенерировать само *N* путем умножения двух больших простых чисел *P* и *Q*, так что простые факторы *N* мы уже знаем. Для числа, которое имеет только два простых фактора (как в нашем случае), функция Эйлера равна:

J(N) = (P-1)(Q-1)

Теперь мы выбирает некоторое число *E*, которое является простым относительно *J(N)* (зачем нам это условие мы увидим ниже). Нам надо найти *D*, которое является обратным к *E* по отношению к операции возведения в степень по модулю *N*. Это можно сделать, зная *J(N)*.

Имеется правило в модульной арифметике, гласящее, что если операция *возведения в степень* использует модуль *N*, то показатели экспонент должны использовать модуль *J(N)*. Например рассмотрим,

(T^E mod N)^D mod N = T^ED mod N

Оказывается, что умножать показатели степени *E* и *D* мы должны с использованием mod *J(N)*, а **не** mod *N*. Для того, чтобы для заданного показателя шифровки *E* найти подходящее обратное число *D*, нам следует удовлетворить равенство:

T^ED mod N = T
Для этого достаточно, чтобы *ED mod J(N) = 1*, так как *T^1 mod N = T*. Так что проблема нахождения *D* сводится к проблеме нахождения числа, обратного *E* по модулю *J(N)*, что с вычислительной точки зрения тривиально. Следует отметить, что в модульной арифметике есть закон, гласящий, что для заданного модуля *M* число может иметь обратное относительно операции умножения по модулю *M* только если *оно является относительно простым* по отношению к *M*. Вот почему мы выбирали *E* как не имеющее общих простых факторов с *J(N)*, так, чтобы у него имелость обратное *D* по модулю *J(N)*. Тривиальные комбинации *E* и *D* (например *E = D*) отбрасываются как неподходящие с точки зрения секретности, и тогда выбираем новое *E*.
Когда мы выбрали значение *N*, и сгенерировали наши ключи *E* и *D*, можно забыть о *P*, *Q* и *J(N)* так как они сделали свое дело. Мы имеем подходящие ключи шифровки и дешифровки *E* и *D*
C = T^E mod N and *T = C^D mod N*
(на самом деле совершенно не важно какой из ключей *D* или *E* считается ключом шифровки). Не зная чисел *P* и *Q* практически невозможно вычислить *J(N)* и, следовательно, найти *D* по заданному *E* при больших значениях *N*, так что шифрование является надежным.
Итоговый список шагов, необходимых для генерации ключа

- Выбираем пару произвольных больших простых чисел *P* и *Q* и находим *N* путем умножения
- Вычисляем функцию Эйлера числа *N*, *J(N)* = (*P*-1)(*Q*-1)
- Выбираем число *E* так, чтобы оно было относительно простым по отношению к *J(N)*
- Находим *D*, обратное число к *E* по отношению к операции умножения по модулю *J(N)*, и тривиальные значени отбраковываем как несекретные (*E=D*)
- Найдя подходящую пару ключей, ключ *E* объявляем открытым и его можно использовать для шифровки сообщений, адресованных владельчу пары *E* и *D*: *C = T^E mod N*
- Ключ *D* держится в секрете и используется для дешифровки полученных сообщений: *T = C^D mod N*

Надежность RSA

Факторизация *N* приведет к вскрытию алгоритма RSA. Не было *доказано*, что нет полиномиального по затратам времени решения задачи нахождения простых факторов большого числа (то есть возможно, что в будущем будет найден алгоритм, который факторизует *N* достаточно быстро для вскрытия RSA). Однако, несмотря на постоянное продвижение в алгоритмах факторизации, ни один из них не удовлетворяет критерию полиномиальности по времени, что сделало бы проблему RSA разрешимой.
Важно отметить, что не было доказано, что безопасность RSA целиком зависит от проблемы нахождения простых факторов большого числа. Однако все другие способы нахождения *D* по заданному *E* оказались эквивалентны по затратам задаче факторизации *N*. Есть вероятность, что будет найден алгоритм для нахождения *E*-того корня по модулю *N* более простым путем, чем факторизация *N*. Тем не менее, до сих пор не был найден такой алгоритм и RSA выдержал огромное число попыток вскрытия.

Методические материалы, определяющие процедуру оценивания выполнения практических работ

Описание методики оценивания выполнения практических работ: оценка за выполнение тестовых заданий ставится на основании знания теоретического материала по теме практической работы, умений и навыков применения знаний на практике, работы с оборудованием, анализировать результаты практической работы.
Критерии оценки (в баллах*):*
- 5 баллов выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется полное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются умения и навыки работы с оборудованием, применения

знания на практике, анализа результатов практической работы и формулирование выводов, владение навыками прикладной деятельности;
- **4** балла выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, имеются пробелы в знании применяемых методик исследования; демонстрируется неполное знание фактического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются некоторые недостатки умения работать с оборудованием, применять знания на практике, недостатки владения навыками прикладной деятельности и способности анализировать результаты практической работы, формулировать выводы, прослеживать причинно-следственные связи;
- **3** балла выставляется студенту, если демонстрируются неполные знания цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется неполное, несистемное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются заметные недостатки в умении работать с оборудованием, применять знания на практике, недостаточно владеет навыками прикладной деятельности, способностью анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи;
- **0-2** балла выставляется студенту, если демонстрируются полное или почти полное отсутствие знания цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется полное или почти полное отсутствие знания теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются значительные недостатки умения работать с оборудованием, применять знания на практике, владения навыками прикладной деятельности, способности анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи.

Групповой опрос

1. Уровни формирования режима информационной безопасности
2. Нормативно-правовые основы информационной безопасности в РФ
3. Ответственность за нарушения в сфере информационной безопасности
4. Антивирусные программы
5. Правила защиты от компьютерных вирусов
6. Специфика средств защиты в компьютерных сетях

Методические материалы, определяющие процедуру оценивания группового вопроса

В процессе проведения занятия задаются вопросы по темам, как текущего занятия, так и по предыдущим.
Студент, правильно отвечающий на вопрос, получает дополнительный балл.
Студент, неправильно ответивший на вопрос, не получает дополнительный балл.

Лабораторная работа

Лабораторная работа № 4
«Защита информации в сети»

Цель работы: Усвоить основные требования к защите вычислительной сети.

Содержание отчета
1. Название и цель работы;
2. Индивидуальное задание согласно варианту;
3. Выполнение индивидуального задания;
4. Ответы на контрольные вопросы.

Методические указания

Каждая сеть нуждается в защите от преднамеренного или случайного повреждения. В то же время хороший администратор сети всегда помнит, что при обеспечении безопасности надо знать меру, надо строить защиту таким образом чтобы люди не испытывали трудности при выполнении своей работы. Наибольшую угрозу для безопасности сети представляют:

· несанкционированный доступ;

· электронное подслушивание:

· кража:

· преднамеренное или неумышленное повреждение.

Уровень защиты сети зависит от ее назначения. Например, сеть, которая хранит данные крупного банка, требует более мощной защиты, чем локальная сеть, соединяющая компьютеры небольшой общественной организации.

Разработка политики защиты. Для защиты сети необходимо проводить определенную политику, т.е. следовать набору правил и предписаний. Выработка политики безопасности (security policy) - первый шаг, который должна сделать любая организация, обеспечивая защиту своих данных. Политика устанавливает "генеральную линию", опираясь на которую и администратор, и пользователи будут вносить изменения, находить выход из нештатных ситуаций при развитии сети..

*Упреждающая защита. Л*учшая политика защиты данных имеет предупредительный характер. Предотвращая несанкционированный доступ или действия, Вы сохраните информацию. Однако система, основанная на упреждении, требует, чтобы администратор в совершенстве владел средствами и методами, которые помогают сохранить данные в безопасности.

Аутентификация. Перед тем как получить доступ к сети, Вы должны ввести правильные имя пользователя и пароль. Поскольку пароли связаны с учетными записями пользователей, система идентификации паролей является первой линией обороны против несанкционированного доступа.

Обучение. Маловероятно, что хорошо обученный пользователь сети непреднамеренно повредит данные. Администратор должен научить пользователей сети всем тонкостям работы и методам безопасности. Для этого он может составить короткое, ясное руководство, а в случае необходимости - организовать обучение, особенно новых пользователей.

Физическая защита оборудования. Обеспечение безопасности данных надо начинать с физической защиты оборудования. На степень физической защиты влияют:

· размер компании;

· характер информации;

· доступные ресурсы;

В одноранговых системах организованная политика защиты оборудования часто отсутствует, так как пользователи сами отвечают за безопасность своих компьютеров и данных.

Защита серверов. В больших централизованных системах, где число индивидуальных пользователей достаточно велико, а данные компании имеют важное значение, серверы должны быть физически защищены от случайного или преднамеренного вмешательства. Простейшее решение -запереть серверы в специальном помещении с ограниченным доступом. Но не все организации имеют такую возможность. А вот закрыть серверы хотя бы в кабинете или в большом шкафу смогут все.

Модели защиты.

Защитив физические компоненты сети, администратор должен гарантировать, что сетевые ресурсы находятся в безопасности от несанкционированного доступа и от случайного или преднамеренного уничтожения. Политика назначения привилегий и прав на доступ к сетевым ресурсам - основа для превращения сети в инструмент успешного ведения бизнеса. Сейчас широко применяются две модели, которые обеспечивают безопасность информационных и аппаратных ресурсов:

· защита через пароль:

· защита через права доступа.

Эти модели называют также защитой на уровне совместно используемых ресурсов (resource level) (защита через пароль) и защитой на уровне пользователя (user level) (защита через права доступа).

Пароль доступа к ресурсам. Один из методов защиты совместно используемых ресурсов - присвоить пароль каждому общедоступному ресурсу. Таким образом, доступ к ресурсу осуществляется только в том случае, когда пользователь вводит правильный пароль. Во многих системах ресурсы могут быть предоставлены в совместное использование с разными типами прав доступа. В Windows, например, к каталогам может быть доступ только для чтения, полный доступ и доступ в зависимости от пароля.
- Доступ только для чтения (read only).
- Полный доступ (full access).
- Доступ в зависимости от пароля (depending on password). Доступ в зависимости от пароля заключается в следующем. Совместно используемому каталогу присваивается пароль двух уровней: доступ только для чтения и полный доступ. Сотрудники, знающие пароль доступа для чтения, могут лишь читать данные, а те, кто знает пароль полного доступа, имеют соответственно полный доступ. Защита совместно используемых ресурсов паролем - самый простой метод защиты, который позволяет любому, кто знает пароль, получить доступ к нужному ресурсу.

Права доступа. Защита через права доступа заключается в присвоении каждому пользователю определенного набора прав. При входе в сеть пользователь вводит пароль. Сервер, проверяя комбинацию имени пользователя и пароля, т.е. проверяя права пользователя в базе данных безопасности, предоставляет или запрещает доступ к сетевым ресурсам.

Защита с применением прав доступа обеспечивает более высокий уровень управления доступом к совместно используемым ресурсам, а также более строгий режим безопасности, чем защита паролем. Так как защита на уровне пользователя более эффективна и может определять различные уровни безопасности, большие организации обычно отдают предпочтение именно этой модели.

Защита ресурсов. Проверив и подтвердив имя и пароль пользователя, система безопасности сети предоставляет ему доступ к соответствующим ресурсам. Однако иметь пароль еще недостаточно - для доступа к ресурсам нужны права.

Следующая таблица отражает стандартные права доступа, присваиваемые совместно используемым каталогом или файлам.

Право	Значение
Read	Чтение и копирование файлов из совместно используемого каталога
Execute	Запуск (выполнение) программ из каталога
Write	Создание новых файлов в каталоге
Delete	Удаление файлов в каталоге
No Access	Запрещение на доступ к каталогу, файлу, ресурсу

Права группы. Обязанность администратора - присвоить каждому пользователю соответствующие права доступа к каждому ресурсу. Наиболее эффективный способ решить эту задачу - через группы, особенно в крупных организациях с большим количеством пользователей и ресурсов. Windows для установки групповых прав доступа к каталогам и файлам использует File Manager. Сначала администратор оценивает, какие права необходимы каждому пользователю, а затем включает пользователей в соответствующие группы. Этот метод назначения прав намного удобнее, чем присвоение отдельных прав каждому пользователю.

Аудит. Аудит (auditing) - это запись определенных событий в журнал безопасности (security log) сервера. Этот процесс отслеживает действия пользователей в сети. Он выступает как часть защиты сети. поскольку в журнале безопасности отражены имена всех пользователей, которые работали с конкретными ресурсами или пытались получить к ним доступ. Кроме того, он предоставляет информацию для тех подразделений, которые хотят определить (и оплатить) затраты на использование некоторых ресурсов. Аудит фиксирует такие действия, как:

· попытки входа в сеть:

· подключение к указанным ресурсам и отключение от них;
· разрыв соединения;
· блокировка учетных записей;
· открытие и закрытие файлов;
· модификация файлов:
· создание и удаление каталогов;
· модификация каталогов;
· события на сервере и его модификация;
· изменение паролей;
· изменение параметров регистрации;

Аудит показывает, как работает сеть. Администратор может использовать журнал безопасности для подготовки отчетов, где отразит любые заданные действия, а также дату и время их совершения, Например, повторяющиеся неудачные попытки входа в сеть (особенно в необычное время) могут указывать на то. что несанкционированный пользователь добивается доступа к сети.

Бездисковые компьютеры Бездисковые (diskless) компьютеры не имеют приводов гибких или жестких дисков. Они способны выполнять те же задачи, что и компьютеры с дисками, но сохранять данные на локальных гибких или жестких дисках не могут. Поэтому бездисковые компьютеры идеальны в смысле безопасности: пользователи лишены возможности сохранить данные на носителе и забрать его с собой. Бездисковые компьютеры не нуждаются в загрузочных дисках. Они связываются с сервером и входят в сеть с помощью специальных загрузочных ПЗУ, установленных на платах сетевого адаптера. При включении бездискового компьютера загрузочная ПЗУ сигнализирует серверу, что компьютер собирается стартовать. Сервер реагирует на сигнал, передавая загрузочное программное обеспечение в оперативную память бездискового компьютера и автоматически посылая пользователю приглашение войти в сеть. Как только пользователь входит в сеть. компьютер подключается к ней.

Шифрование данных. Утилита шифрования (encryption) данных кодирует информацию перед тем, как передать ее по сети. Когда данные поступят на соответствующий компьютер, они будут декодированы в понятную форму с помощью ключа - кода для дешифровки закодированной информации. Усовершенствованные схемы шифрования автоматизируют и шифрование, и дешифрование. Лучшие системы шифрования основаны на специальной аппаратуре, их стоимость очень высока. Традиционный стандарт шифрования - Data Encryption Standard (DES). Он описывает спецификации ключа и способ шифрования. Как отправителю, так и получателю информации необходим доступ к ключу. Существует только один способ передать ключ из одного места в другое - сообщить его. Здесь сразу же возникают проблемы, которые делают DES уязвимым. Учитывая это, был разработан и новый стандарт, называемый Commercial COMSEC Endorsement Program (CCEP). Он призван заменить DES.

Защита от вирусов. Разрабатывая систему защиты сети, необходимо принимать во внимание и вирусы. К сожалению, ни одна антивирусная программа не может полностью устранить угрозу их проникновения; в основном эти программы борются с последствиями вирусного "нашествия":

Лучший метод борьбы с вирусами - исключить возможность несанкционированного доступа.

Защита данных.

К числу бедствий можно отнести все, что влечет за собой потерю данных в сети. Причины бедствий самые разнообразные: от дел рук человеческих до природных катаклизмов, в том числе: воровство или вандализм; пожар; отказы источников питания и скачки напряжения: отказы компонентов; природные явления, такие, как молнии, наводнения, бури и землетрясения.

Остановка сети, вызванная чрезвычайными причинами, всегда бедствие, всегда серьезное уменьшение производительности, Требуется время на восстановление данных из хранилища резервных копий. Существуют методы и системы. предупреждающие катастрофическую потерю данных:

· резервное копирование на магнитную ленту;
· источники бесперебойного питания (UPS);
· отказоустойчивые системы.

Могут использоваться все эти системы или любая из них, в зависимости от ценности данных и бюджета организации.

Резервное копирование на магнитную ленту. Наиболее простой и недорогой метод предупредить катастрофическую потерю данных - периодическое резервное копирование с последующим хранением копий за пределами организации.

Система резервного копирования. Общее правило гласит: если Вы не можете в дальнейшем обойтись без чего-то, сделайте его резервную копию. Выбор объектов для резервного копирования - целые диски, отдельные каталоги или файлы - зависит от того, насколько быстро нужно продолжить работы после потери важных данных, восстановив их. Полное резервное копирование может ускорить восстановление конфигурации диска, однако, если имеются большие объемы данных, требует значительного числа дополнительных магнитных лент. Резервирование отдельных файлов и каталогов потребует меньше лент, однако администратору придется вручную восстанавливать конфигурацию диска. Критические данные должны резервироваться ежедневно, еженедельно или ежемесячно, в зависимости от степени их важности и от того, насколько часто они обновляются. Самое лучшее время для резервного копирования - время наименьшей загрузки системы..

Методы резервного копирования. Эффективная политика резервирования использует комбинацию методов, которые приведены в следующей таблице

Метод	**Описание**
Полное копирование	Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
Копирование	Копирование всех выбранных файлов без отметки о резервном копировании
Резервное копирование с приращением	Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования
Ежедневное копирование	Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Дифференцированное резервное копирование	Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

Методы резервного копирования обычно применимы к накопителям на магнитной ленте. Для резервного копирования больших объемов данных лучше всего использовать несколько отдельных лент при циклическом расписании. Ленты можно использовать в многонедельном цикле (в зависимости от количество . В первый день цикла администратор выполняет полное резервное копирование, а в последующие дни выполняет резервирование с приращением. Когда цикл полностью завершен, процесс начинается снова. Некоторые администраторы пришли к выводу: целесообразно выполнять несколько резервирований с приращением каждый день в установленное время.

Журнал резервного копирования. Ведение журнала окажет существенную помощь при последующем восстановлении файлов. Копии журнала должны храниться вместе с магнитными лентами, рядом с компьютерами.

Источник бесперебойного питания Источник бесперебойного питания (UPS) - это автоматический внешний источник энергии, который поддерживает работоспособность сервера или других устройств в случае сбоев электрической сети. Системы бесперебойного питания используют способность источников бесперебойного питания взаимодействовать с операционной

системой через специальный интерфейс. Стандартная система бесперебойного питания обеспечивает две важнейшие для сети функции: питание сервера в течение некоторого времени; управление безопасным завершением работы системы.
Источником энергии обычно служат аккумуляторы. При нарушении питания UPS извещает пользователей о сбое и предупреждает их о необходимости завершить работу. При этом хорошо организованная система бесперебойного питания будет предотвращать доступ к серверу дополнительных пользователей, а также пошлет администратору сети сообщение об аварии. UPS обычно размешается между сервером и источником питания.
Отказоустойчивые системы Отказоустойчивые системы защищают данные, дублируя и размещая их на различных физических носителях (например, на разных дисках). Избыточность (redundancy) данных позволяет осуществлять к ним доступ даже в случае выхода из строя части системы. Избыточность - общий отличительный признак большинства отказоустойчивых систем. Тем не менее отказоустойчивые системы нельзя использовать как замену регулярного резервного копирования серверов и локальных жестких дисков. Отказоустойчивые системы предлагают следующие варианты для обеспечения избыточности данных:
· чередование дисков;
· зеркализацию дисков;
· замену секторов.
Избыточные массивы недорогих дисков. Типы отказоустойчивых систем стандартизованы и классифицируются по уровням. Эти уровни выступают как избыточные массивы недорогих дисков (RAID). Они предлагают различные комбинации производительности, надежности и стоимости. Windows содержит программную поддержку технологии RAID (уровней 0,1 и 5).
Уровень 0 - чередование дисков. При чередовании дисков (disk striping) данные делятся на блоки размером 64Кб и равномерно распределяются по всем дискам массива. Однако чередование дисков не обеспечивает повышенной надежности, так как не создает избыточности данных. При повреждении любого раздела будут потеряны все данные. Чередование дисков объединяет множество областей неформатированного свободного пространства в один большой логический диск, распределяя хранилище данных по всем дискам одновременно. В Windows NT для чередования дисков необходимо как минимум два физических диска (максимальное число - 32 диска). При чередовании дисков можно использовать разделы дисков нескольких типов: SCSI, ESDI и IDE. Чередование дисков имеет ряд преимуществ. Во-первых, несколько малых разделов образуют один большой раздел, благодаря чему лучше используется дисковое пространство. Во-вторых, применяя несколько дисковых контроллеров, можно резко увеличить производительность.
Уровень 1 - зеркализация дисков. Зеркализация дисков (disk mirroring) - дублирование раздела и запись его копии на другом физическом диске. Поэтому всегда есть две копии данных, причем каждая - на отдельном диске. Любой раздел может быть зеркализирован. Эта стратегия - простейший метод защиты одиночного диска от сбоев. Зеркализация дисков выступает как форма непрерывного резервного копирования, так как при этом поддерживается полная копия раздела с другого диска.
Дублирование. Дублирование диска (disk duplexing) - это пара зеркальных дисков, каждым из которых управляет отдельный контроллер. При этом уменьшается трафик через единичный контроллер (увеличивается быстродействие). Дублирование предназначено для защиты не только от сбоев носителей, но и от отказов контроллеров.
Уровень 2 - чередование дисков с записью кода коррекции ошибок. Блок данных - при записи - делится на части, распределяемые по разным дискам. Одновременно генерируется код коррекции ошибок (ECC), который также записывается на разных дисках. Для кода коррекции ошибок требуется больше дискового пространства, чем при методе с контролем четности. Хотя последний гораздо эффективнее использует дисковое пространство, он уступает в этом отношении уровню 5.
Уровень 3 - код коррекции ошибок в виде четности. Чередование дисков с использованием кода коррекции ошибок, хранящимся в четности, подобно уровню 2. Контролем четности называют процедуру проверки ошибок, при которой устанавливается количество единиц в каждой переданной группе битов. Оно должно быть одинаковым - четным или несчетным. В этом случае

говорят, что данные переданы без ошибок. При этой стратегии метод с кодами ECC заменяется схемой контроля четности, которой необходим только один диск для хранения информации контроля четности. Это приводит к тому, что примерно 85 процентов дискового пространства используется для хранения непосредственно данных.

Уровень 4 - чередование дисков большими блоками. Эта стратегия, основанная на методе чередования дисков, обеспечивает запись цельных блоков данных на каждый диск в массиве. Отдельный контрольный диск используется для хранения информации о четности. При каждой записи соответствующая информация о четности должна быть прочитана с контрольного диска и модифицирована. Из-за высоких накладных расходов этот метод больше подходит для операций с крупными блоками, чем для обработки транзакций.

Уровень 5 - чередование с контролем четности. В настоящее время чередование с контролем четности - наиболее популярный метод построения отказоустойчивых систем. Уровень 5 поддерживает от 3 до 32 дисков и распределяет информацию о четности по всем дискам массива (по всему набору чередования). Данные и информация об их четности всегда размещаются на разных дисках. Блок информации о четности записывается в каждой полосе (ряде) чередования распределенной по дискам. Информация о четности помогает восстановить данные с отказавшего физического диска. Если отказал один диск, для полного восстановления данных достаточно информации, распределенной по оставшимся дискам. RAID4 хранит блок четности на одном физическом диске, тогда как RAID5 распределяет информацию о четности равномерно по всем дискам.

Замена секторов. Некоторые операционные системы предлагают дополнительную возможность для обеспечения отказоустойчивости. Она называется замена секторов (sectorsparing) или "горячая замена" (hot fixing). Эта возможность заключается в автоматическом восстановлении секторов во время работы компьютера. Если при операции дискового ввода вывода обнаружен дефектный сектор, отказоустойчивый драйвер попытается переместить данные на хороший сектор, а дефектный пометить как "bad". Если перенос данных прошел успешно, драйвер не сообщает файловой системе о сбое. Замена секторов невозможна для ESDI- и IDE-дисков.

Некоторые сетевые операционные системы имеют утилиты, которые извещают администратора обо всех сбоях секторов, а также об угрозе потери данных, если избыточная копия также будет потеряна.

Использование помехоустойчивых кодов для обнаружения ошибок передачи данных в сети

Сигналы, непосредственно передаваемые по линиям связи, подвержены влиянию ряда факторов, воздействие которых может привести к возникновению ошибок в принятой информации. Некоторые из ошибок могут быть обнаружены на основании анализа вида принятого сигнала. Реальным способом снижения ошибок при приеме данных является введение избыточности в передаваемую информацию. В системах передачи информации без обратной связи данный способ реализуется в виде помехоустойчивого кодирования.

Помехоустойчивое кодирование предполагает введение в передаваемое сообщение, наряду с информационными, так называемых проверочных разрядов. Избыточность позволяет отличить разрешенную и запрещенную (искаженную за счет ошибок) комбинации при приеме, иначе одна разрешенная ситуация переходила бы в другую.

Помехоустойчивый код характеризуется тройкой чисел (n, k, d_0), где n – общее число разрядов в передаваемом сообщении, включая проверочные (r), k=n-r - число информационных разрядов, d_0 - минимальное кодовое расстояние между разрешенными кодовыми комбинациями, определяемое как минимальное число бит в этих комбинациях. Число обнаруживаемых (t_0) и (или) исправляемых ($t_и$) ошибок (разрядов) связано с параметром d_0 соотношениями:

$d_{0>=} t_0 + 1$ $d_{0>=} 2t_и + 1$ $d_{0>=} t_0 + t_и + 1$

Существующие помехоустойчивые коды можно разделить на ряд групп: блочные и непрерывные. Блочные делятся в свою очередь на равномерные (n=const) и неравномерные (код Морзе). Равномерные делятся на разделимые и неразделимые. Разделимые делят на систематические (линейные) и нелинейные.

К систематическим относят: биты четности|-нечетности; циклические; коды БЧХ. Только систематические линейные коды используются для обнаружения ошибок в передаваемых сообщениях.
Наибольшее распространение из них получили коды: **Хэмминга, циклический и итеративный.** Такие коды составляются по определенному правилу. Сначала определяется число контрольных символов m, соответствующих числу k информационных символов. В кодовой комбинации к информационным символам добавляются контрольные, которые обычно располагаются на местах кратных степени 2, то есть 1, 2, 4, 8 местах и т.д. Далее, пользуясь проверочной таблицей, присваивают контрольным символам значение 0 или 1. При приеме кодовой комбинации ошибку обнаруживают и исправляют с помощью проверки на четность.
Циклическим называют групповой код, в котором все комбинации связаны дополнительным условием цикличности. В циклических кодах, как и кодах Хэмминга, информационные и контрольные символы всегда расположены на определенных местах, что позволяет легко обнаруживать и исправлять ошибки. Перспективными с точки зрения аппаратурной реализации представляются коды БЧХ (Боуза-Чаудхури-Хотвингема).

Контрольные вопросы

1. В чем заключается политика безопасности сети?
2. Что представляет наибольшую угрозу безопасности сети?
3. В чем заключается физическая защита оборудования сети?
4. Модели защиты сети?
5. Что такое аудит?
6. Для чего используется шифрование?
7. В чем заключается защита от вирусов?
8. Как осуществляется защита данных от потерь?
9. Методы резервного копирования информации?
10. Назначение и уровни RAID-массивов?

Задание

Заполните пропуски в следующих высказываниях
1. Обеспечение безопасности данных надо начинать с защиты сетевого _____.
2. Модель защиты на основе прав доступа имеет и другое название - защита на_____
3. Защита ресурсов паролем заключается в назначении пароля доступа каждому совместно используемому _____.
4. Защита через права доступа заключается в присвоении каждому пользователю некоторых
5. Наиболее эффективный способ присвоить права доступа - использование ____.
6. Аудит - это запись определенного типа событий в _____ сервера для отслеживания действий пользователей в сети.
7. Бездисковые компьютеры связываются с сервером и входят в сеть с помощью специальной загрузочной микросхемы ПЗУ, установленной на _____ компьютера.
8. Чтобы выполнять резервное копирование, необходимо иметь регулярное _____.
9. Ведение _____ всех резервных копирований очень важно для последующего восстановления файлов.
10. Отказоустойчивые системы защищают данные, дублируя и размещая их на различных _____ носителях.
11. При использовании технологии RAID уровня 0, называемой _____. данные делятся на блоки размером 64 Кб и равномерно распределяются по всем дискам массива с фиксированными частотой и порядком.
12. Чередование дисков уровня 0 не обеспечивает _____ данных.
13. _____ дисков - дублирование раздела и запись его копии на другом физическом диске, поэтому всегда есть две копии данных.
14. Дублирование предназначено для защиты не только от сбоев носителя, но и от отказов ____.

15. Запись блоков данных на каждый диск массива называется _____ дисков.

Методические материалы, определяющие процедуру оценивания лабораторных работ

Описание методики оценивания выполнения лабораторных работ: оценка за выполнение тестовых заданий ставится на основании знания теоретического материала по теме лабораторнjq работы, умений и навыков применения знаний на практике, работы с оборудованием, анализировать результаты лабораторной работы.

Критерии оценки (в баллах*):*

- **5** баллов выставляется студенту, если демонстрируются знания темы, цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется полное знание теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются умения и навыки работы с оборудованием, применения знания на практике, анализа результатов лабораторной работы и формулирование выводов, владение навыками прикладной деятельности;
- **4** балла выставляется студенту, если демонстрируются знания темы, цели и задач лабораторной работы, хода работы, имеются пробелы в знании применяемых методик исследования; демонстрируется неполное знание фактического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются некоторые недостатки умения работать с оборудованием, применять знания на практике, недостатки владения навыками прикладной деятельности и способности анализировать результаты лабораторной работы, формулировать выводы, прослеживать причинно-следственные связи;
- **3** балла выставляется студенту, если демонстрируются неполные знания цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется неполное, несистемное знание теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются заметные недостатки в умении работать с оборудованием, применять знания на практике, недостаточно владеет навыками прикладной деятельности, способностью анализировать результаты лабораторной работы и формулировать выводы, прослеживать причинно-следственные связи;
- **0-2** балла выставляется студенту, если демонстрируются полное или почти полное отсутствие знания цели и задач лабораторной работы, хода работы, применяемых методик исследования; демонстрируется полное или почти полное отсутствие знания теоретического материала по теме лабораторной работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются значительные недостатки умения работать с оборудованием, применять знания на практике, владения навыками прикладной деятельности, способности анализировать результаты лабораторной работы и формулировать выводы, прослеживать причинно-следственные связи.

Зачет

Зачет является оценочным средством для всех этапов освоения компетенций.

Примерные вопросы к зачету, 5 курс / 10 семестр

1. Понятие информации, ее свойства.
2. Надежность информации.
3. Понятие информационного ресурса.
4. Классификация информационных ресурсов
5. Информационные ресурсы в современных условиях.
6. Понятие об информационной безопасности.
7. Категории информационной безопасности.
8. Информационная безопасность человека и общества.
9. Методы обеспечения информационной безопасности.
10. Правовое обеспечение информационной безопасности в РФ.

11. Основные угрозы информационной безопасности для государства, человека, информационной системы.
12. Защита информации. Основные понятия, направления организации защиты информации.
13. Характеристика основных методов защиты информации.
14. Организационные меры защиты информации.
15. Программно-технические меры защиты информации.
16. Правовые меры защиты информации.
17. Практика применения методов и средств защиты информации.
18. Характеристика основных средств защиты информации.
19. Угрозы компьютерной безопасности.
20. Типы вредоносных программ. Борьба с ними.
21. Защита операционных систем.
22. Защита программного обеспечения.
23. Аутентификация пользователей.

Методические материалы, определяющие процедуру оценивания зачета

Зачет выставляется по рейтингу, в зависимости от эффективности работы в процессе изучения дисциплины, что определяется количеством набранных баллов за все виды заданий текущего и рубежного контроля
зачтено – от 60 до 110 баллов
не зачтено – от 0 до 59 баллов.

1.3. Рейтинг-план дисциплины

Таблица перевода баллов текущего контроля в баллы рейтинга

	5	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**
0	0	0	0	0	0	0	0	0	0	0
1	5	3	2	2	1	1	1	1	1	1
2		5	4	3	2	2	2	2	2	1
3			5	4	3	3	3	2	2	2
4				5	4	4	3	3	3	2
5					5	5	4	4	3	3
6						5	5	4	4	3
7							5	5	4	4
8								5	5	4
9									5	5
10										5

Рейтинг-план дисциплины представлен в Приложении 1.

2. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Информационная безопасность : Учеб. для студ. вузов, обуч. по гуман. и соц .-эконом. спец. / В. И. Ярочкин .— 5-е изд. — М. : Гаудеамус: Академический Проект, 2008 .— 543 с.
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях : учеб. пособие — Электрон. дан. — М.: ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032

Дополнительная литература

1. Нечаев, Д.Ю. Надежность информационных систем [Электронный ресурс] : учебное пособие / Д.Ю. Нечаев, Ю.В. Чекмарев. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 64 с. — Режим доступа: https://e.lanbook.com/book/3030
2. Информационная безопасность компьютерных систем и сетей: учеб. пособ. для студ. учрежд. сред. проф. образ., обуч. по группе спец. 2200 "Информатика и вычислит. техника" / В. Ф. Шаньгин .— М. : Форум: ИНФРА-М, 2010 .— 415 с.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Режим доступа: https://elibrary.ru/.
2. Электронная библиотечная система «Лань» [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/.
3. Университетская библиотека онлайн biblioclub.ru [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/.
4. Электронная библиотека УУНиТ [Электронный ресурс]. – Режим доступа: https://elib.bashedu.ru/.
5. Российская государственная библиотека [Электронный ресурс]. – Режим доступа: https://www.rsl.ru/.
6. Национальная электронная библиотека [Электронный ресурс]. – Режим доступа: https://xn--90ax2c.xn--p1ai/viewers/.
7. Национальная платформа открытого образования npoed.ru [Электронный ресурс]. – Режим доступа: http://npoed.ru/.
8. Электронное образование Республики Башкортостан [Электронный ресурс]. – Режим доступа: https://edu.bashkortostan.ru/.
9. Информационно-правовой портал Гарант.ру [Электронный ресурс]. – Режим доступа: http://www.garant.ru/.

Программное обеспечение

1. Браузер Google Chrome - Бесплатная лицензия https://www.google.com/intl/ru_ALL/chrome/privacy/eula_text.html
2. Система дистанционного обучения Moodle - Бесплатная лицензия http://www.gnu.org/licenses/gpl.html
3. Office Professional Plus - Договор №0301100003620000022 от 29.06.2020, Договор № 2159-ПО/2021 от 15.06.2021, Договор №32110448500 от 30.07.2021
4. Программа моделирования сетей NetEmul - Бесплатная лицензия http://netemul.sourceforge.net/help/en/intro.html
5. Файловый менеджер DoubleCommander - Бесплатная лицензия https://sourceforge.net/projects/doublecmd/
6. Windows - Договор №0301100003620000022 от 29.06.2020, Договор № 2159- ПО/2021 от 15.06.2021, Договор №32110448500 от 30.07.2021
7. Браузер Яндекс, сервисы яндекс: метрика, wordstat - Бесплатная лицензия https://yandex.ru/legal/browser_agreement/index.html ссылка на лицензию https://yandex.ru/legal/metrica_mobile_agreement/index.html
8. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 - Бесплатная лицензия https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html
9. Браузер Яндекс - Бесплатная лицензия https://yandex.ru/legal/browser_agreement/index.html

10. Справочно-правовая система «Гарант» - Договор №52 от 20.03.2019, Договор №35 от 23.03.2020, Договор №69 от 15 марта 2021,Договор 53 от 16.03.2022 Договор №31 от 16 марта 2023г.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория 301 Читальный зал (электронный каталог)(ФМ)	Для самостоятельной работы	Компьютеры в сборе, учебная мебель, принтер samsung, сканер hp scanyet g2410. Программное обеспечение 1. Браузер Google Chrome 2. Office Professional Plus
Аудитория 313(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации	Экран, компьютеры в комплекте, учебная мебель, доска классная, интерактивная доска , принтер canon mf-3228 (принтер+копир+сканер), проектор optoma x316. Программное обеспечение 1. Система дистанционного обучения Moodle 2. Программа моделирования сетей NetEmul 3. Windows 4. Браузер Яндекс, сервисы яндекс: метрика, wordstat 5. Браузер Яндекс 6. Браузер Google Chrome 7. Office Professional Plus 8. Файловый менеджер DoubleCommander 9. Справочно-правовая система «Гарант»
Аудитория 313 а(ФМ)	Для хранения оборудования	Оверхед-проектор "reflex" с кейсом.
Аудитория 411(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации	Экран настенный 180*180 screenmedia, проектор benq mx505, учебная мебель, компьютеры в сборе. Программное обеспечение 1. Файловый менеджер DoubleCommander

		2. Система дистанционного обучения Moodle 3. Программа моделирования сетей NetEmul 4. Программа для симулирования и планирования сети GraphicalNetworkSimulator 3 5. Браузер Яндекс 6. Браузер Google Chrome 7. Office Professional Plus
Аудитория 420(ФМ)	Для самостоятельной работы	Компьютеры в сборе, нетбук lenovo, принтер canon lbp3010b, учебная мебель. Программное обеспечение 1. Office Professional Plus 2. Windows 3. Браузер Google Chrome