Приложение 2 к РПД Защита информации
01.03.02 Прикладная математика и информатика
направленность (профиль)
Системное программирование
и компьютерные технологии
Форма обучения – очная
Год набора – 2022

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

1. Общие сведения

1.	Кафедра	Математики, физики и информационных технологий
2.	Направление подготовки	01.03.02 Прикладная математика и информатика
3.	Направленность (профиль)	Системное программирование и компьютерные технологии
4.	Дисциплина (модуль)	Б1.О.16.03 Защита информации
5.	Форма обучения	Очная
6.	Год набора	2022

2. Перечень компетенций

– **ОПК-4**: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

3. Критерии и показатели оценивания компетенций на различных этапах их формирования

Этапы формирования компетенций (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	**Уметь:**	**Владеть:**	
Введение в информационную безопасность (ИБ). Уровни обеспечения ИБ.	ОПК-4	• о существующих средствах защиты информации и возможностях их использования в задачах создания и внедрения информационных систем; • принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа	• проводить анализ степени защищённости информации; • осуществлять повышение уровня защиты с учётом развития математического и программного обеспечения вычислительных систем	• навыками применения современных алгоритмов для шифрования/ дешифрования секретной информации • навыками решения практических задач профессиональной деятельности	Лабораторные работы 1, 6 Контрольные задания
Криптографическая защита данных.					Лабораторные работы 2, 3, 4 Контрольные задания
Защита информации в компьютерных сетях.					Лабораторные работы 2, 5 Контрольные задания
Современные технологии защиты информации.					Лабораторные работы 5, 6 Контрольные задания
Законодательство РФ в области защиты данных и обеспечения ИБ.					Лабораторная работа 1 Контрольные задания

Шкала оценивания в рамках балльно-рейтинговой системы:

«неудовлетворительно» – 60 баллов и менее; «удовлетворительно» – 61-80 баллов; «хорошо» – 81-90 баллов; «отлично» – 91-100 баллов

4. Критерии и шкалы оценивания

Отчет о выполнении лабораторной работы:

Содержание отчета	Балл
Все упражнения и задания лабораторной работы выполнены полностью и своевременно, все материалы оформлены в соответствии с требованиями	10
Данная оценка выставляется в следующих случаях: – выполнено не менее 60% упражнений и заданий лабораторной работы – требования к оформлению материалов соблюдены частично – работа выполнена полностью, но представлена после установленных сроков сдачи	5
Задания лабораторной работы не выполнены, выполнены неудовлетворительно либо невозможно установить авторство	0

Подготовка доклада, участие в учебной дискуссии:

Критерии оценивания текста доклада	0-5 баллов
Выполнены все требования к содержательной и оформительской части доклада: – текст доклада соответствует теме, тема раскрыта достаточно полно, сделаны необходимые выводы и обобщения, теоретические сведения проиллюстрированы примерами – доклад оформлен в соответствии с требованиями к оформлению – при подготовке доклада использовано не менее трех источников	5
При оформлении текста доклада допущены недочеты, не влияющие на его содержательную часть	2
Оценка выставляется, если: – тема доклада раскрыта слабо или неполно – в тексте отсутствуют выводы, обобщения, приведены частные примеры – оформление текста не соответствует требованиям	1
Оценка выставляется, если: – текст доклада не представлен – тема доклада не раскрыта, либо из текста можно сделать вывод о том, что студент не разобрался в материале – текст в значительной мере заимствован из одного или нескольких источников – оформление текста не соответствует требованиям	0
Критерии оценивания выступления	0-5 баллов
Выполнены все требования к публичной защите доклада: – во время выступления использованы наглядные материалы (презентация, иллюстрации, схемы) – ответы на уточняющие вопросы демонстрируют понимание студентом темы, аргументированы и подкреплены как теоретическими сведениями, так и практическими примерами	2
Ответы на вопросы неполны либо отсутствуют	1
Выступления нет либо оно проведено неудовлетворительно	0

Контрольное (экзаменационное) тестирование: балл рассчитывается пропорционально количеству верно решенных дидактически единиц (модулей):

Количество верно решенных ДЕ	0-5	6	7
Количество баллов	По 5 баллов за каждую ДЕ	32	40

Типовые контрольные задания и методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Типовое контрольное тестовое задание

Задание № 1. ДЕ-1 Элементы теории чисел
С помощью алгоритма быстрого модулярного возведения в степень вычислить: $4^{811} \pmod{101}$.
Вычисления оформить в виде таблицы.

Задание № 2. ДЕ-2 Криптосистемы с секретным ключом
Используя скремблер с начальным состоянием key = 011_2 и фиксированными разрядами − первым и третьим, по заданной входной последовательности бит 01001_2 получить выходную последовательность.

Задание № 3. ДЕ-3 Криптосистемы с открытым ключом
С помощью алгоритма RSA расшифровать сообщение (6; 30; 31; 24), если p = 3, q = 11, a = 7,
причём каждая буква русского алфавита для простоты представлена своим номером в алфавитном порядке и передаваемый блок информации m соответствует одной букве.

Задание № 4. ДЕ-3 Криптосистемы с открытым ключом
По алгоритму Эль-Гамаля, с набором ключей p = 31, y = 10, x = 9,
а) выступая в роли отправителя, поставить электронную подпись под сообщением: m = 5;
б) выступая в роли получателя, проверить электронную подпись.

Задание № 5. ДЕ-4 Вычислительные проблемы криптологии
Используя метод Шенкса (алгоритм малых и больших шагов), относительно неизвестной величины l решить уравнение
$11^l = 59 \pmod{71}$, т.е. вычислить $l = \text{ind}_{11} 59$ по модулю 71.

Образец решения типового контрольного задания
Решение задания № 1. Будем вычислять $z^s \bmod n$ с помощью повторяющихся возведений в квадрат. Задача решается с помощью бинарного представления степени $s = [s_k, s_{k-1}, \ldots s_1, s_0]$.

```
MODULAR-EXPONENTIATION(z, s, n)
d = 1;
for (i= k; i<=0; i– –)
        {       d = (d · d) (mod n);
                if (si == 1) { d = (d · z) (mod n)}
        }
return d
```

Сложность алгоритма. Если z, s, n – l-битные числа, где l=k+1, то арифметических операций требуется O(l), а битовых операций – $O(l^3)$.

Применим данный алгоритм к нашему примеру, в котором: z=4, s=811, n =101.
Сначала переводим степень s=811 в двоичную систему счисления:

$811_{10} = 2^9 + 2^8 + 2^5 + 2^3 + 2^1 + 2^0 = 1100101011_2$.

Как видим, в двоичном представлении степени 811 содержится 10 разрядов.
Начинаем заполнять таблицу. В первую строку помещаем номера разрядов – с 9-го по 0-й. Во вторую строку переписываем поразрядно саму степень. В первую (не заголовочную) ячейку третьей строки помещаем z, т.е. 4.

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4									

Новое значение d определяем следующим образом:
- возводим текущее d в квадрат: 4^2
- и, поскольку s_8=1, ещё домножаем на z, т.е. на 4.

Итого, $4^2 \cdot 4 = 64$.
Так как 64 (mod 101) = 64, записываем 64 в следующую ячейку третьей строки:

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64								

Новое значение d определяем следующим образом:
- возводим текущее d в квадрат: 64^2 (поскольку s_7=0, больше ни на что домножать не надо).

Так как $64^2 \pmod{101} = 56$, записываем 56 в следующую ячейку:

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56							

Определяем следующее значение d:

- возводим текущее d в квадрат: 56^2 (поскольку s_6=0, домножать на z не надо).

Так как $56^2 \pmod{101} = 5$, записываем 5 в следующую ячейку:

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5						

Определяем следующее значение d:

- возводим текущее d в квадрат: 5^2
- и, поскольку s_5=1, ещё домножаем на z, т.е. всё на ту же 4.

Итого, $5^2 \cdot 4 = 100$. Так как $100 \pmod{101} = 100$, то записываем 100 в следующую ячейку:

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100					

Далее, возводим текущее d в квадрат: 100^2 (поскольку s_4=0, домножать на z не надо). Так как $100^2 \pmod{101} = 1$, записываем 1 в следующую ячейку:

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100	1				

- Возводим текущее d в квадрат: 1^2
- и, поскольку s_3=1, ещё домножаем на z, т.е. всё на ту же 4.

Итого, $1^2 \cdot 4 = 4$.

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100	1	4			

Возводим текущее d в квадрат: 4^2 (поскольку s_2=0, домножать на z не надо)

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100	1	4	16		

Затем получим $16^2 \cdot 4 = 14 \pmod{101}$.

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100	1	4	16	14	

И, наконец, $14^2 \cdot 4 = 77 \pmod{101}$.

№ разряда	9	8	7	6	5	4	3	2	1	0
s	1	1	0	0	1	0	1	0	1	1
d	4	64	56	5	100	1	4	16	14	77

Число, полученное в последней ячейке третьей сроки, и является ответом.
Ответ. $4^{811} \pmod{101} =$ **77**.

Решение задания № 2. Для начала вспомним таблицу значения для сложения по модулю 2:

x_1	x_2	$x_1 \oplus x_2$

0	0	0
0	1	1
1	0	1
1	1	0

Записываем входную последовательность 01001 (выделена жёлтым цветом) в третий столбец таблицы вертикально, а ключ 011 (выделен голубым цветом) – в четвёртый столбец горизонтально.

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
	←	0	0	1	1				
		1							
		0							
		0							
		1							

Складывая по модулю 2 первый символ входной последовательности и самый левый символ скремблера (выделены жёлтым цветом), в первом столбце получаем первый символ выходной последовательности (выделен голубым цветом):

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
		1							
		0							
		0							
		1							

После этого преобразуем скремблер 011 следующим образом:

- складываем по модулю 2 его первый и третий разряды (выделены жёлтым цветом) 0⊕1 = 1;
- дописываем эту единицу в конец скремблера: 0111;
- самый левый разряд скремблера отбрасываем; остаётся 111;
- новое значение скремблера помещаем со сдвигом во вторую строку таблицы:

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
		1		1	1	1			
		0							
		0							
		1							

Далее процесс продолжается аналогичным образом. Складывая по модулю 2 следующий символ входной последовательности и самый левый символ скремблера (выделены жёлтым цветом), в первом столбце получаем следующий символ выходной последовательности (выделен голубым цветом):

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
0	←	1		1	1	1			
		0							
		0							
		1							

- Преобразуем скремблер 111:
- складываем по модулю 2 его первый и третий разряды (выделены жёлтым цветом) 1⊕1 = 0;

• дописываем ноль в конец скремблера: 1110;
• самый левый разряд скремблера отбрасываем; остаётся 110;
• новое значение скремблера помещаем со сдвигом в третью строку таблицы:

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
		1		1	1	1			
		0			1	1	0		
		0							
		1							

Складывая по модулю 2 следующий символ входной последовательности и самый левый символ скремблера (выделены жёлтым цветом), в первом столбце получаем следующий символ выходной последовательности (выделен голубым цветом):

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
0	←	1		1	1	1			
1	←	0			1	1	0		
		0							
		1							

Выход		Вход	Скремблер						
1	**2**	**3**	**4**						
0	←	0	0	1	1				
0	←	1		1	1	1			
1	←	0			1	1	0		
1	←	0				1	0	1	
1	←	1					0	1	0

Итак, выходная последовательность имеет вид:
Ответ: 00111.

Решение задания № 3. Получив секретное сообщение, абонент А расшифровывает его с помощью своего секретного ключа. Найдём этот ключ.
1) Определим $n = p \cdot q = 3 \cdot 11 = 33$.
2) Найдем $\varphi(n) = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$.
3) Данное значение: $a = 7$, в самом деле, взаимно простое с $\varphi(n) = 20$.
4) Составим уравнение $ax = 1 \pmod{(\varphi(n))}$: $7x \equiv 1 \pmod{(20)}$
и решим его с помощью алгоритма Евклида.

7	=	20·0	+	7
20	=	7·2	+	6
7	=	6·1	+	1
6	=	1·6	+	0

k	0	1	2	3
q_k	0	2	1	6
P_k	0	1	1	7
S_k	1	2	3	20

Окончательно $x = (-1)^2 S_2 = 3$.

К каждой компоненте данного вектора применяем формулу: $m_2 = m_1^x \pmod{n}$.

$m_1^{(1)} = 6$; $m^{(1)} \equiv 6^x \pmod{n} = 6^3 \pmod{33}$;
$m_1^{(2)} = 30$; $m^{(2)} \equiv 30^x \pmod{n} = 30^3 \pmod{33}$;
$m_1^{(3)} = 31$; $m^{(3)} \equiv 31^x \pmod{n} = 31^3 \pmod{33}$;
$m_1^{(4)} = 24$; $m^{(4)} \equiv 24^x \pmod{n} = 24^3 \pmod{33}$.

Для вычисления сравнений воспользуемся алгоритмом быстрого модулярного возведения в степень. Поскольку показатель степени во всех четырёх сравнениях одинаков ($x = 3_{10} = 11_2$), вычисления можно оформить в одной таблице.

№ разряда	1	0	
s	**1**	**1**	
d_1	6	$6^2 \cdot 6 \equiv 18 \pmod{33}$	18 → «Р»
d_2	30	$30^2 \cdot 30 \equiv 6 \pmod{33}$	6 → «Е»
d_3	31	$31^2 \cdot 31 \equiv 25 \pmod{33}$	25 → «Ч»
d_4	24	$24^2 \cdot 24 \equiv 30 \pmod{33}$	30 → «Ь»

Ответ: РЕЧЬ

Решение задания № 4.
а) Выбрав число k = 13, которое является простым по отношению к
φ(p) = p–1 = 30
находим $u = y^k \bmod p = (10^{13} \bmod 31) = 9$.
Затем, подставляя данные значения m = 5, x = 9, p = 31 и найденное значение u = 9 в уравнение
m = (x·u + k·w) mod (φ(p)), получим уравнение относительно неизвестной величины w:
5 = (9·9 + 13w) (mod 30).
Решая его, найдём: w = 8.
Электронная подпись, таким образом, имеет вид: (u, w) = (9, 8).

б) Определяем $a = y^x \pmod p = 10^9 \pmod{31} = 16$,
после чего проверяем, выполняется ли равенство: $a^u \cdot u^w = y^m \pmod p$.
Вычисляем значение слева: $a^u \cdot u^w = 16^9 \cdot 9^8 = 25 \pmod{31}$;
Вычисляем значение справа: $y^m = 10^5 = 25 \pmod{31}$.
Так как 25 = 25, то подпись верна.
Ответ:
а) (u, w) = (9, 8);
б) $a^u \cdot u^w = y^m \pmod p = 25 \pmod{31}$.

Решение задания № 5. Будем искать неизвестный показатель l уравнения

$$b^l = a \pmod q, \tag{1}$$

в виде

$$l = i*m - j, \tag{2}$$

где

$$m = [\sqrt{q}\,] + 1, \tag{3}$$

i = 1, 2, …, m; j = 0, 1, …, m.
Заменив в уравнении (1) неизвестную величину l по формуле (2) на выражение
$i*m - j$, получим $b^{im - j} = a \pmod q$,
откуда

$$b^{im} = a*b^{j} \pmod q. \tag{4}$$

В соответствии с алгоритмом Шенкса, предварительно вычисляем ряд (“большие шаги”)

$$b^m, b^{2m}, b^{3m}, \ldots, b^{mm}, \tag{5}$$

который содержит все возможные значения **левой** части уравнения (4), а также ряд (“малые” шаги)

$$a, a*b^1, a*b^2, a*b^3, \ldots, a*b^m, \tag{6}$$

который содержит все возможные значения **правой** части этого уравнения.

Затем ищем такой элемент $a*b^j$ ряда (6), который совпадает с каким-нибудь элементом b^{im} ряда (5), и по известным значениям i и j с помощью формулы (2) определяем l.

В процессе работы алгоритма в среднем выполняется 1.5 $\sqrt{q}$ операций, в худшем случае требуется 2 $\sqrt{q}$

операций, т.е. его сложность имеет порядок $\sqrt{q}$.

В нашем примере: b = 11, a = 59.

1) По формуле (3) определяем m: $m = [\sqrt{q}\,] + 1 = [\sqrt{71}\,] + 1 = 9$.

2) Составляем ряд: $b^m, b^{2m}, b^{3m},..., b^{mm}$:

$b^m \pmod q = 11^9 \pmod{71} = 61$;

$b^{2m} \pmod q = b^m \cdot b^m \pmod q = 61 \cdot 61 \pmod{71} = 29 \pmod{71}$;

$b^{3m} \pmod q = b^m \cdot b^{2m} \pmod q = 61 \cdot 29 \pmod{71} = 65 \pmod{71}$;

$b^{4m} \pmod q = b^m \cdot b^{3m} \pmod q = 61 \cdot 65 \pmod{71} = 60 \pmod{71}$;

$b^{5m} \pmod q = b^m \cdot b^{4m} \pmod q = 61 \cdot 60 \pmod{71} = 39 \pmod{71}$;

$b^{6m} \pmod q = b^m \cdot b^{5m} \pmod q = 61 \cdot 39 \pmod{71} = 36 \pmod{71}$;

$b^{7m} \pmod q = b^m \cdot b^{6m} \pmod q = 61 \cdot 36 \pmod{71} = 66 \pmod{71}$;

$b^{8m} \pmod q = b^m \cdot b^{7m} \pmod q = 61 \cdot 66 \pmod{71} = 50 \pmod{71}$;

$b^{9m} \pmod q = b^m \cdot b^{8m} \pmod q = 61 \cdot 50 \pmod{71} = 68 \pmod{71}$.

Для наглядности поместим элементы ряда в таблицу 1, пронумеровав их, начиная с 1:

Таблица 1

i	1	2	3	4	5	6	7	8	9
b^{im}	61	29	65	60	39	36	66	50	68

3) Составляем ряд: $a, a*b^1, a*b^2, a*b^3, ..., a*b^m$.

Можно не вычислять ВСЕ элементы этого ряда; вычисления продолжаем до тех пор, пока не получим такое число, которое присутствует во второй строке таблицы 1.

$a \pmod q = 59$;

$a*b^1 \pmod q = 59 \cdot 11 \pmod{71} = 10 \pmod{71}$;

$a*b^2 \pmod q = b \cdot (a \cdot b^1) \pmod{71} = 11 \cdot 10 \pmod{71} = 39 \pmod{71}$

$a*b^3 \pmod q$ и последующие элементы ряда можно не вычислять.

Поместим элементы ряда в таблицу 2, пронумеровав их, на этот раз начиная с **0**:

Таблица 2

i	0	1	2	3	4	5	6	7	8
$a*b^j$	59	10	39	…	…	…	…	…	…

4) В таблице 1 элемент 39 имеет номер 5, следовательно, i = 5.
В таблице 2 элемент 39 имеет номер 2, следовательно, j = 2.
Зная i и j, по формуле (2) определяем искомое значение l: $l = i*m–j = 5*9–2 = 43$.

5) Чтобы сделать проверку, вычисляем 11^{43} по модулю 71; убеждаемся, что $11^{43} = 59 \pmod{71}$.
Ответ: 43.

Вопросы к экзамену

1 Основные определения: информация, защищаемая информация, безопасность информации, три основные угрозы безопасности, защита информации, направления защиты информации.
2. Методы защиты от несанкционированного доступа
3. Стандарт «Критерии оценки безопасности информационных технологий» («Общие критерии» ISO/IEC 15408). Функциональные требования. Требования доверия
4. Классификация криптоалгоритмов: по типу преобразований, по типу использования ключей, по размеру преобразуемого блока

5. Одноалфавитные подстановки. Многоалфавитные подстановки. Перестановки по ключу.
6. Симметричные криптоалгоритмы. Скремблеры, как пример поточного шифра.
7. Симметричные криптоалгоритмы. Сеть Фейстеля и её применение в блочных шифрах.
8. Китайская теорема об остатках и её применение в криптографии.
9. Алгоритм быстрого модулярного возведения в степень. Оценка сложности алгоритма.
10. Несимметричные криптоалгоритмы. Обмен ключами по алгоритму Диффи-Хеллмана. Протокол для двух участников. Протокол для большего числа участников.
11. Несимметричные криптоалгоритмы. Криптосистема RSA: генерация ключей, шифрование, дешифрование. Требования к набору ключей.
12. Несимметричные криптоалгоритмы. Криптосистема Эль-Гамаля: генерация ключей, шифрование, дешифрование.
13. Электронная подпись. Создание и проверка подписи в криптосистеме Эль-Гамаля.
14. Временная метка (Timestamp): создание и проверка временной метки.
15. Разделение секрета. Способы разделения секрета.
16. Простое число. Псевдопростое число. Способы нахождения больших простых чисел. Алгоритм Миллера-Рабина.
17. Задача факторизации и её решение методом силовой атаки. Функция Эйлера.
18. Метод Полларда для решения задачи факторизации.
19. Метод Ферма для решения задачи факторизации.
20. Порядок числа. Дискретный логарифм (индекс числа). Задача вычисления дискретного логарифма и её решение методом силовой атаки.
21. Метод согласования (Сильвера-Полига-Хеллмана) для решения задачи вычисления дискретного логарифма.
22. Метод малых и больших шагов (Шенкса) для решения задачи вычисления дискретного логарифма.
23. Эллиптическая кривая. Эллиптическая группа. Сложение и умножение на число в эллиптической группе.
24. Обмен ключами, шифрование и дешифрование с использованием эллиптических кривых.
25. Технологии аутентификации. Простая аутентификация. Строгая аутентификация. Протоколы строгой аутентификации. Основные атаки на протоколы аутентификации.
26. Технологии межсетевых экранов (МЭ). Функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Дополнительные возможности МЭ.
27. Технологии виртуальных защищенных каналов и сетей VPN. Концепция построения виртуальных защищенных сетей. VPN. VPN-решения для построения защищенных сете. Достоинства применения технологий VPN.
28. Технологии обнаружения вторжений Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак: методы анализа сетевой информации, классификация систем обнаружения атак IDS, компоненты и архитектура IDS, методы реагирования.
29. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты: классификация компьютерных вирусов, жизненный цикл вирусов, основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети.