



/ 27004—
2021

,

,

▪

(ISO/IEC 27004:2016, IDT)



2021

1 « » « » () -
) « - » (,
 4
 2 022 « »
 3 19 2021 . 388-
 4 / 27004:2016 « -
 » (ISO/IEC 27004:2016 «Infor-
 mation technology — Security techniques — Information security management — Monitoring, measurement,
 analysis and evaluation». IDT).
 / 27004 27 «
 » () 1 « » () -
 5 / 27004—2011
 6 , 4. -
 29 2015 . 162- « 26
) « 1
 — « », « ».
 () «
 ». ,
 —
 (www.gost.ru)

ISO. 2016 —

© IEC. 2016 —

© . 2021

1	1
2	1
3	1
4	1
5	2
5.1	2
5.2	/ 27001	3
5.3	3
5.4	3
6	4
6.1	4
6.2	4
6.3	5
6.4	6
6.5	6
7	7
7.1	7
7.2	7
7.3	8
8	8
8.1	8
8.2	9
8.3	10
8.4	12
8.5	13
8.6	13
8.7	14
8.8	14
8.9	14
()	15
()	17
()	44
	45

()²⁾

9.1 / 27001 , -

-

-

27000. , -

-

-

-

-

-

/ 27001. -

-

/ 27001.

Information technology. Security techniques. Information security management.
Monitoring, measurement, analysis and evaluation

— 2021—11—30

1

，
（ ）
9.1 / 27001.
：
；
（ ），
；
，

2

3

8

/ 27000.

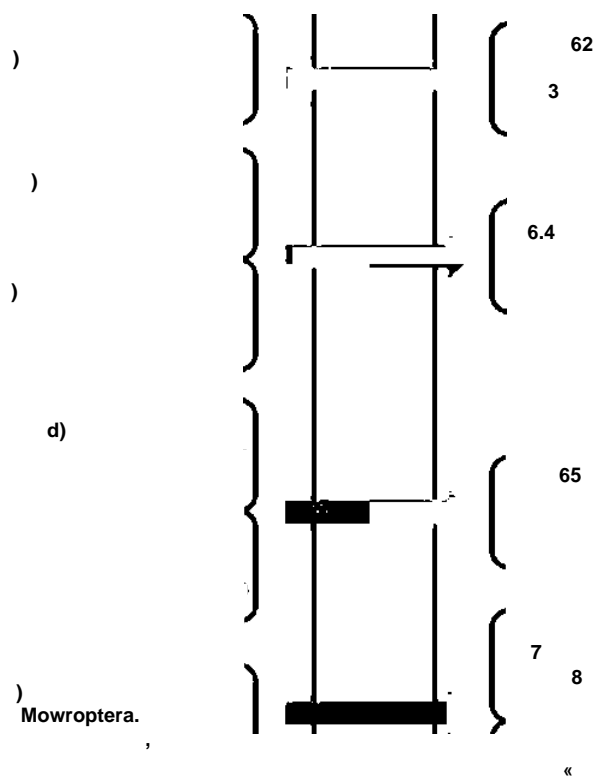
：
-
-
/。
（IEC Electropedia）：
<http://www.iso.org/obp>;
[httpJ/www.electropedia](http://www.electropedia).

4

：
- 5;
- 6;
• 7;
- 8.
9.1 / 27001. 1.

/ 27001:2013. 9.1

/ 27004:2016



« »* »
«
*« . ,
»
«
»

1 —

9.1 / 27001

9.1 / 27001.

1.

5

5.1

/ 27001.

5.2 / 27001

9.1 / 27001

7

9.1 / 27001

-

;

*

*

*

*

*

9.1 / 27001

1.

(. 8.9).

,

9.1 / 27001

,

,

, (. 6.4).

5.3

(. 9.1)

/ 27001)

,

,

.

,

.

,

,

:

-

,

,

,

;

-

,

,

.

-

;

-

,

,

.

,

:

-

.

,

,

,

.

5.4

.

.

,

,

,

:

-

:

:

.

,

:

-

:

;

/ 27001

6

6.1

6.2

- a)
- b)
- c)
- d)
- e)
- f)
- g)
- h)
- i)
- j)
- k)
- l)
-)

(.).

6.3

8

8

d)

10.1

/

27001,

8.

1»:

-

-

-

-

-

-

-

-

«

(

).

/

27001

/

27001.

/

27010).

j)

k)

()

330

15.05.2010 .,

239

(25.12.2017

. 12.7 «

*).

27001

(9.1 5.3 / 27001)

b) $\frac{1}{2}$; $\frac{1}{2}$,

d)

f) _____ ; _____ ,

;

7

7.1

» 9.1 / 27001 « » -

7.2

100 %.

9.1 / 27001
(. 7.3).
1)

7.3

a)

b)

c)

d)

e)

f)

)

h)

3

4

8

8.1

2

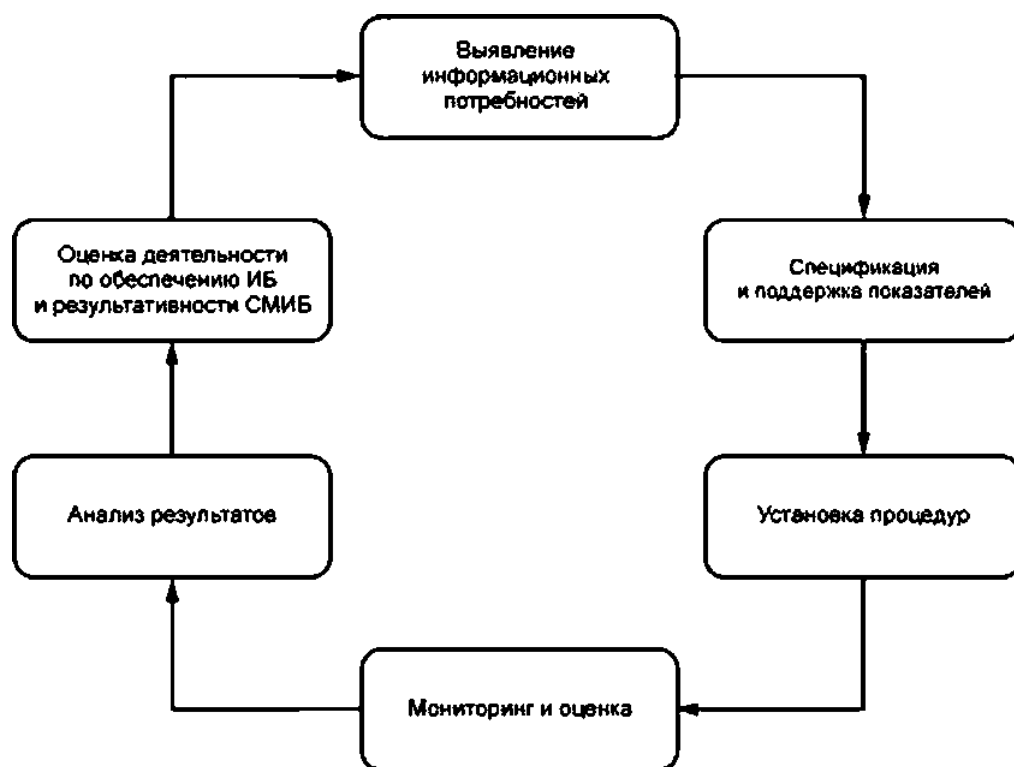
)

)

)

)
)
)
 0

(. 8.8).



2 —

8.2

a)
 b)
 c)
 d)

e)

1)
 2)
 3)

0

1)
 2)
 3)
 4)

5) ; ,

6) ; ,

) ; , -

h) . -

8.3

8.3.1

a) :
b) ;
c) , ,

d) - ;
) - ;

f) -
:

) , ,

:
h) ,

o ;
j) ;

k) . -

8.3.2

a) ;
b) :
c) ;
d) .

8.3.3

a) ;
b) ;
c) ;
d) ;
)
f) / -
)

i)

j)

k)

1)

)

)

,

)

(

)

1.

1.

(. 1).

1).

1 —

	»
-	
-	
	’ ’ , « », « », « » « »
/	—
	’ ’ “ ”
-	’ ’ “ ”
	“ ”
	“ ”
	’ ’ “ ”

1

	<p>—</p> <p>—</p>
	<p>—</p> <p>—</p>

8

8.3.4

6.4.

8.3.5

8.4

a)

b)

8.7

5.2

)

)

8.8

a)

b)

c)

d)

8.9

9.1 / 27001,

a)

b)

c)

d)

()

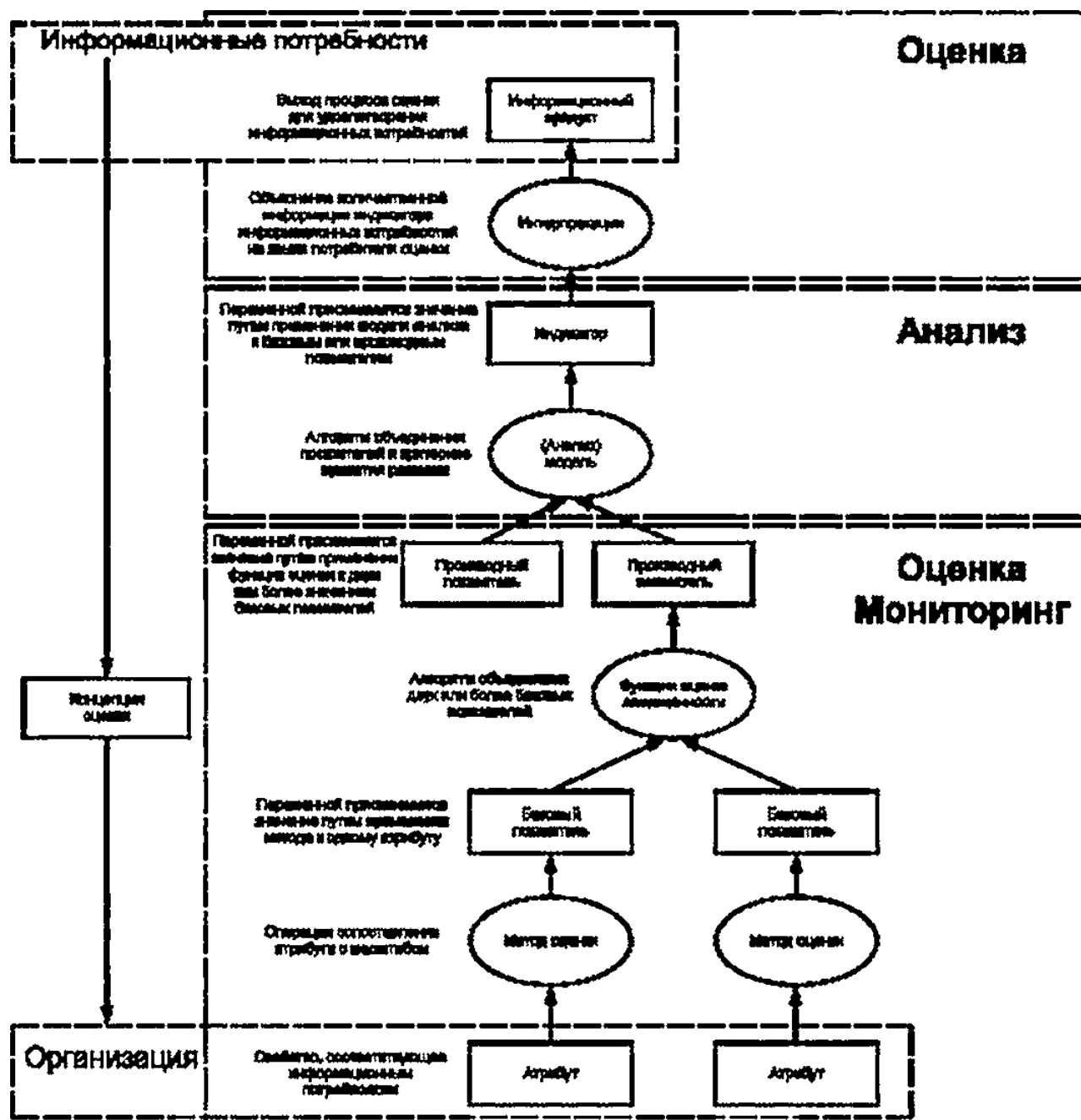


Рисунок А.1 — Ключевые отношения в информационной модели оценки

()

.1

/ 27001

(> 27001)	
5.1. 7.1	.2
7.5.2, .5.1.2	.
5.1. 9.3	.4
8.2. 8.3	.5
9.2. .18.2.1	.6
10	.7
10	.8
10. .16.1.6	.9
10.1	.10
.7.2	.11
.7.2.2	.12
.7.2.1. .7.2.2	.13
.7.2.2	.14 -
.7.2.2. .9.3.1, .16.1	.15
.9.3.1	.16 ,
.9.3.1	.17 ,
.9.2.5	.18
.11.1.2	.19
.11.1.2	.20
.11.2.4	.21
.12.1.2	.22
.12.2.1	.2
.12.2.1	.24
.12.2.1. .17.2.1	.25
.12.2.1. .13.1.3	.26
. 12.4.1	.27
. 12.6.1	.28
. 12.6.1. . 18.2.3	.29

*	
-	,
/	() » 100) (, -
	: > 80 %. > = 40 %. < 40 %
-	-
	:) (, :
-	: , - : : :-
	, ,

∴ / 27001:2013. 5.1.2:

/ 27001:2013, 7.5.2:

.4

-	
-	-
	:
/	[] [-];
	0,7 1.1.): 0.5; ,): , , , - -

-	<p>1.1 , :</p> <p>1.2 > :</p> <p>2.1.1 :</p> <p>2.1.2 , :</p> <p>2.1.3 , :</p> <p>2.2 -</p>
	<p>:</p> <p>:</p> <p>:</p> <p>2 :</p>
-	<p>:</p> <p>); (</p> <p>:</p> <p>:</p> <p>:</p> <p>:</p> <p>:</p> <p>-</p>
	:
-	<p>,</p> <p>-</p> <p>.</p>

∴ / 27001:2013, 9.3:

/ 27001:2013, 5.1:

.5

-	
-	
	:
/	!
	:
	1
-	
	:

-	: ; :
	:

∴ / 27001:2013. 6.2:
/ 27001:2013, 8.3:

.6

-	
-	
/	()*(
) * 100
	>95%
-	
-	: ; : ; :
	,

∴ / 27001:2013. 9.2:
/ 27001:2013. 18.2.1:

.7

-	
-	
	, () ; (-)

	»
/	((, ()] 100
	90%
-	
-	: : : ; :
	(,) ,

∴ / 27001:2013, 10:
— , (, ,).
.

.8

-	
-	,
	,
/	()
	,
-	
	: : - : ; ;
	- ∴ • • (-

∴ / 27001:2013. :

	<p>0.0 2)) ()) 0.4 0.0 0.2</p> <p>,</p> <p>.</p> <p>,</p>
-	<p>1. ,</p> <p>2. ,</p> <p>3. , -</p>
	<p>:</p> <p>:</p> <p>:</p> <p>:</p> <p>1</p>
	<p>:</p> <p>:</p> <p>:</p> <p>:</p> <p>-</p>
	<p>,</p> <p>,</p> <p>,</p> <p>-</p> <p>,</p>

.; / 27001:2013, 10.1:

.11

-	
	<p>,</p> <p>-</p>
	<p>,</p> <p>-</p>
/	<p>11 = [(,)] « 100; (-</p> <p>.</p> <p>12 = [(,)] * 100</p> <p>8</p>
	<p>:</p> <p>> 90 12 > 50 %</p> <p>:</p> <p>> 60% 12 > 30 %</p> <p>:</p> <p>—</p> <p>,</p> <p>-</p> <p>.</p> <p>—</p> <p>-</p> <p>—</p>

-	/ : *
	: , : : :
	: — : — , .
	, , -
	, : , -

∴ / 270012013. 7.2: .
.12

-	
-	-
	-
/	((,)(,)])» 100
	0—60 % — : 60—90 % — : 90—100 %- 10 %. — , - — - —
-	« * / -

	<p> 1.1. 1.2. 2.1. 2.2. </p>

∴ / 27001:2013, 7.2.2: ()

/ 27001:2013, .7.2.1:

.14 -

-	
-	3 - -
	3 - -
/	3 3 .
	3 : 90—100 % ; : 60—90 % . : < 60 %
-	/ : :
	: :
	: ; : ; :

	,
	, *

∴ / 27001:2013. 7.2.2: , ()

.15

-	
-	,
	, , -
/	$= (\quad , \quad)$ $= 1 - (\quad)$ $= (\quad)$ $d =$
	d: 0—60: : 60—80: : 90—100:
-	,
	: — , -
	: ;
	: - , :
	- () ;
	, ,

∴ / 27001:2013, 16.1: ;
 / 27001:2013. 9.3.1: ;
 / 27001:2013, 7.2.2 , ()

.16 ,

-	
-	,
	a) b)
/	a) b) c) d)
	0.9; 0.8 0.9. 0.8.
-	1 2

∴ / 27001:2013. 9.3.1:

.17 ,

-	
-	-
	1 2

	»
	: : -; :
	, , , ,
	-

∴ / 27001:2013. 9.2.5:

.19

-	
-	, , -
/	0 5: 0 : 1 , PIN- (); 2 , - 3 (); PIN- ; - 4 + : 5 PIN- , (, (. .)
	3
-	, : • ; • PIN- ; • : •
	: : : : 12 ; : 12
	, ; : / ; :

∴ / 27001:2013, 11.1.2:

.20

-	
-	1 2 :
	(,) -
/	- / : (, ,) - -
	1.0
-	-
	: : : ; : . -
	;
	-

∴ 27001:2013, .11.1.2:

—

,

-

.

.21

-	
-	
/	[]
	, , , ; - 0.9; 0;

-	; ; ;
	: ;
	: ; ;
	1 / 2
	, - ;

∴ / 27001:2013. 11.2.4:

.22

-	
-	,
	,
/	(,)(-)
-	, , , , -
	: ;
	: ;
	, , , , -
	-

∴ / 27001:2013, 12.1.2:

.23

-	
-	
	,
/	((,) ,
	, -
-	1 , 2 ,
	: : : : : ; : : : 1 ;
	; ;
	;
	,

.; / 27001:2013, 12.2.1:

.24

-	
-	，
	，
	， (，)
/	()()

	0 ,
-	
	: ; : ; : -
	(, .)

∴ / 27001:2013. 12.2.1: -

8.25

-	
-	- -
	- - (,)
/	(())
-	-
	: ; : ; : -
	: , () - ; (),

∴ / 27001:2013. 17.2.1;

.26

-	
-	

	»
/	0 ,
	0
-	
	: / - ; : / ; : / -
	,
	, -

∴ / 27001:2013. .13.1.3:

.27

	»
-	
-	-
	-
/	(, /] " 100
	20 % -
-	, -
	: (, -): , - : (,); : : 2 ; : 2
	: ; : , ; : , -
	: ;
	, -

/ / 27001:2013. .12.4.1:

.28

	»
-	
-	,
	(),
/	{ : - , : - , , - : - , / : - . .
	100%
-	: ; - ;
	: 3 :
	: : : : -
	: ; -
	: ;

∴ / 27001:2013. . 12.6.1:

.29

-	
-	, , - (,),
	,
/	[:] 100; ; 100 %; : >= 75 %; : <75%

	(—)
-	, , -
	: ;
	: ; ;
	: , ;
	: - ;
	,
	-

∴ / 27001:2013. 2.6.1:

/ 27001:2013. .18.2.3:

-	
-	
	()
/	(, CVSS)* -
-	
	: »
	: ;
	: ;
	;
	, Unix . .) (/

/ / 27001:2013. .12.6.1:

	»
	1 2, 0.9;
-	,
	: : : : : 2 ; : 2
	; ; ; ;
	, . -

∴ / 27001:2013. 15.1.2:
.32

-	
-	
	,
/	a) : b) - ; c) ,
-	
	: : : : : ;
	: ; ; ; ;

	: ; : -

∴ / 27001:2013. .16:

.

	»
-	
-	;
	(,): (,)
/	- 6 ; : < 1.0; : 1.00—1.30; : > 1.3. 1 2
-	
	:): : ; :— , -
	-
	-
	:

∴ / 27001:2013. .16.1:

8.34

	»
-	
-	,
	,

/	,
	,
-	
	: ;
	: ; -
	: ; , -
	, -

.; / 27001:2013. .16.1.3:
.35

-	
-	-
/	{ }] (-
	0.6 0.8 1.1. -
-	1 2
	: ; : ; : ; : ; 2 ; : 2
	: , : ; : , .
	;
	, -

/ / 27001:2013. .18.2.1:

.36

-	
-	
	, / -
/	(, ()
	1
-	
	: ; : : :
	: ;
	-

∴ / 27001:2013. .18-2.3:

()

.1 « » —

« » , -

, (S1) -

(). S2 — , -

(,).

S3 — , S2. -

. (S3).

, , -

S4P — , -

S4F — , -

S5P — ,

S5F — ,

1 = S1 - S2 — , -

2 = S4P/(S4P * S4F) — (

).

= S5P/(S5P * S5F) — , -

4 = / 2 —

S1 — S2 , ,

- . , -

, -

-

, , -

, ,

, ,

, .

- [1] ISO/TR 10017. Guidance on statistical techniques for ISO 9001:2000
- [2] ISO/IEC 15939. Systems and software engineering — Measurement process
- [3] ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary
- [4] ISO/IEC 27001:2013. Information technology — Security techniques— Information security management systems — Requirements
- [5] NIST Special Publication 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008.
<http://csrc.ntst.gov/publications/nistpubs/800-55Rev1/SP800-55-rev1.pdf>

351.864.1:006.354

35.040

:
(),
,
,
().
-

21.05.2021

08.06.2021.

60*84%.

. . . 5.58. .- . . 5,02.

,

«

»

117418

-, . 3t. . 2.

www.goslinfo.ru info@gostinfo.ru