МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра информационной безопасности

ПРАКТИЧЕСКАЯ РАБОТА №3

по дисциплине «Основы информационной безопасности»

Тема: «Проведение анализа и оценки возможностей реализации угроз информационной безопасности на объекте по методике С.В. Вихорева»

Студентка гр. 0361 _____ Солонухина А.Л.

Преподаватель _____ Воробьёв Е.Г.

Санкт-Петербург
2022

Постановка задачи

1. Описываемая область выбирается на основе собранных материалов по конкретному предприятию, организации или компании.
2. Цель работы: Изучение вида работ по разработке модели угроз, ее актуализации.
3. Отчет выполняется в форме описанной в 1 части методики.

1. Описание предприятия ОУ ВО «НГУ» (Некий ГУ)

Предприятие «НГУ» расположено:

в центре Европейской части России,

в спокойных метеорологических, сейсмических и гидрологических условиях,

не имеющий в непосредственной близости предприятий, и других техногенных сооружений.

«НГУ» имеет гетерогенную, иерархическую корпоративную информационную сеть со счетным количеством (до 20 000) пользователей, которая:

- обрабатывает информацию с разной степенью конфиденциальности
- имеет равенство приоритетов целей ИБ
- пользователи имеют разные права доступа к информации
- сопряженную с сетью Internet

Воздействия источников угроз приносят максимальный ущерб субъекту отношений, а сами источники угроз имеют максимальные возможности по реализации угроз.

2. Выбор приоритетов целей ИБ

Анкета для получения исходных данных по оценке приоритетности целей ИБ

	Содержание вопроса	Да	Нет
1	Может ли несанкционированное разглашение защищаемых сведений:		
1.1	⇒ привести к срыву реализации стратегических планов развития организации, повлиять на снижение ее деловой активности	да	
1.2	⇒ привести к разглашению секретов организации или третьих лиц, ноу-хау, персональных данных, нарушить тайну сообщений	да	
1.3	⇒ повлиять на ухудшение взаимоотношений с партнерами, снижение престижа и деловой репутации организации	да	
	Сумма положительных («Да») ответов по п.1, ∑(«Да») = **(Кп)к**	3	
2	Может ли несанкционированное изменение защищаемой информации:		
2.1	⇒ привести к принятию ошибочных решений (или непринятию вообще), важных для практической деятельности организации	да	
2.3	⇒ привести к полной или частичной дезорганизации деятельности организации или ее подразделений, нарушить взаимоотношения с партнерами	да	
2.4	⇒ изменить содержание персональных данных или другие сведения, затрагивающие интересы личности		нет
	Сумма положительных («Да») ответов по п.2, ∑(«Да») = **(Кп)ц**	2	
3	Может ли задержка в получении защищаемой информации или ее неполучение:		
3.1	⇒ привести к невозможности выполнения взятых организацией обязательств перед третьим лицами	да	
3.2	⇒ привести к несвоевременному принятию решений (или непринятию вообще), важных для практической деятельности организации	да	
3.3	⇒ привести к полной или частичной дезорганизации деятельности организации или ее подразделений	да	
	Сумма положительных («Да») ответов по п.1, ∑(«Да») = **(Кп)д**	3	

Коэффициенты приоритетности целей ИБ

Цели ИБ	$(К_П)_r$
Конфиденциальность	**3**
Целостность	**2**
Доступность	**3**
$(К_П)_c$ = Const = 2	

3. Ранжирование угроз ИБ

Принимая во внимание выбранные приоритеты целей ИБ, и нормированные весовые коэффициенты угроз $(К_В)_k$, считаем коэффициенты актуальности каждой из угроз $(К_А)_k$:

$$(K_А)_k = \frac{(K_В)_k \times (K_П)_r}{\sum_{1}^{k} (K_В)_k \times (K_П)_r}$$

$$(K_B)_k = \frac{'(K_B)_k}{\sum_{k=1}^{8} '(K_B)_k}$$

$´(К_В)_1 = 0,65$ $´(К_В)_5 = 0,20$

$´(К_В)_2 = 0,35$ $´(К_В)_6 = 0,60$

$´(К_В)_3 = 0,50$ $´(К_В)_7 = 0,40$

$´(К_В)_4 = 0,30$ $´(К_В)_8 = 0,50$

Коэффициенты актуальности угроз ИБ

k	Угрозы ИБ	$(К_А)_k$
1	Хищение (копирование) информации и средств ее обработки	**0,22**
2	Утрата (неумышленная потеря, утечка) информации и средств ее обработки	**0,12**
3	Модификация (искажение) информации	**0,11**
4	Отрицание подлинности информации	**0,07**
5	Навязывание ложной информации	**0,04**
6	Уничтожение информации и средств ее обработки	**0,2**
7	Блокирование информации	**0,13**
8	Создание условий для реализации угрозы ИБ	**0,11**

Для рассматриваемого варианта, с учетом формулы

$$\delta_k = 0,2 \times \max\{'(K_В)_k\} = 0,13$$

$\delta_k = 0,2 * 0,65 = 0,13$

Тогда такие угрозы, как:

- «утрата (неумышленная потеря, утечка) информации и средств ее обработки» $(К_А)_2 = 0,12 < 0,13$
- «модификация (искажение) информации» $(К_А)_3 = 0,11 < 0,13$
- «отрицание подлинности информации» $(К_А)_4 = 0,07 < 0,13$
- «навязывание ложной информации» $(К_А)_5 = 0,04 < 0,13$
- «создание условий для реализации угрозы ИБ» $(К_А)_8 = 0,11 < 0,13$

в дальнейшем анализе могут не рассматриваться, как маловероятные.

4. Ранжирование групп источников угроз ИБ

Величины весовых коэффициенты групп источников угроз ИБ (***Kg**i*) и соответствующих им нормированных весовых коэффициентов группы источников угроз ИБ (***Kg**i*)N исходя из формул

$$(Kg_i)_N = \frac{Kg_i}{\sum_1^{g_i}(Kg_i)}$$

$$Kg_i = \sum (K_A)_k$$

и «Таблограммы взаимосвязи угроз, источников, методов реализации угроз ИБ» приведены в таблице:

Весовые коэффициенты групп источников ИБ при равенстве приоритетов целей

g	Код	Группа источников угроз ИБ	***Kg**i*	(***Kg**i*)N
1	[I.A.0]	Антропогенные внешние источники	**0,88**	**0,26**
2	[I.B.0]	Антропогенные внутренние источники	**0,93**	**0,28**
3	[II.A.0]	Техногенные внешние источники	**0,55**	**0,16**
4	[II.B.0]	Техногенные внутренние источники	**0,55**	**0,16**
5	[III.A.0]	Стихийные внешние источники	**0,44**	**0,13**

5. Ранжирование источников угроз ИБ

k_1 – показатель возможности возникновения источника угрозы (1..5)

k_2 – показатель готовности источника угрозы (1..5)

k_3 – коэффициент фатальности применения источника угрозы (1..5)

Коэффициент опасности **$(K_{оп})_i$** для отдельного *источника угроз* рассчитывается по формуле

$$(K_{оп})_i = \frac{\prod_{n=1}^{3}(k_n)_i}{\prod_{n=1}^{3}\max\{(k_n)_i\}} \times (Kg_i)_N$$

Ориентировочная оценка степени опасности источников угроз ИБ

Код (i)	Источники угроз информационной безопасности	$(k_1)_i$	$(k_2)_i$	$(k_3)_i$	$(K_{оп})_i$
[I.A.0]	***Антропогенные внешние источники***	**$(К_1)_N$ = 0,26**			
[I.A.1]	криминальные структуры	**2**	**1**	**4**	**0,02**
[I.A.2]	потенциальные преступники и хакеры	**3**	**3**	**4**	**0,07**
[I.A.3]	недобросовестные партнеры	**1**	**2**	**3**	**0,01**
[I.A.4]	технический персонал поставщиков телематических услуг	**2**	**1**	**5**	**0,02**
[I.A.5]	представители надзорных организаций и аварийных служб	**3**	**2**	**1**	**0,01**
[I.A.6]	представители силовых структур	**3**	**2**	**4**	**0,05**
[I.B.0]	***Антропогенные внутренние источники***	**$(К_2)_N$ = 0,28**			
[I.B.1]	основной персонал (пользователи, программисты, разработчики)	**3**	**5**	**4**	**0,13**
[I.B.2]	представители службы защиты информации (администраторы)	**3**	**3**	**2**	**0,04**
[I.B.3]	вспомогательный персонал (уборщики, охрана)	**2**	**1**	**2**	**0,01**
[I.B.4]	технический персонал (жизнеобеспечение, эксплуатация)	**3**	**2**	**2**	**0,03**
[II.A.0]	***Техногенные внешние источники угроз***	**$(К_3)_N$ = 0,16**			
[II.A.1]	средства связи	**4**	**2**	**3**	**0,03**
[II.A.2]	сети инженерных коммуникации (водоснабжения, канализации)	**4**	**1**	**2**	**0,01**
[II.A.3]	транспорт	**2**	**1**	**1**	**0,00**

[II.B.0]	***Техногенные внутренние источники угроз***	**$(К_4)_N$ = 0,16**			
[II.B.1]	некачественные технические средства обработки информации	**4**	**4**	**5**	**0,10**
[II.B.2]	некачественные программные средства обработки информации	**5**	**5**	**5**	**0,16**
[II.B.3]	вспомогательные средства (охраны, сигнализации, телефонии)	**4**	**3**	**3**	**0,05**
[II.B.4]	другие технические средства, применяемые в учреждении	**2**	**3**	**3**	**0,04**
[III.A.0]	***Стихийные внешние источники***	**$(К_5)_N$ = 0,13**			
[III.A.1]	пожары	**4**	**5**	**5**	**0,10**
[III.A.2]	землетрясения, провалы, обвалы, оползни	**2**	**1**	**5**	**0,01**
[III.A.3]	наводнения, сели, лавины,	**1**	**1**	**4**	**0,00**
[III.A.4]	ураганы, снегопады, метели, штормы	**1**	**2**	**3**	**0,01**
[III.A.5]	магнитные бури	**2**	**2**	**2**	**0,01**
[III.A.6]	радиоактивное излучение	**1**	**1**	**2**	**0,00**
[III.A.7]	различные непредвиденные обстоятельства	**2**	**2**	**2**	**0,01**
[III.A.8]	необъяснимые явления	**2**	**3**	**2**	**0,01**
[III.A.9]	другие форс-мажорные обстоятельства	**2**	**3**	**2**	**0,01**

Рассчитаем из формулы

$$\delta_i = 0{,}2 \times \max\{'(Kg_i)_N\}$$

пороговое значение коэффициента опасности источников угроз δ_i = 0,2 * 0,28 = 0,056

Источники угроз ИБ, имеющие код [I.A.1], [I.A.3], [I.A.4], [I.A.5], [I.A.6], [I.B.2], [I.B.3], [I.B.4], [II.A.1], [II.A.3], [II.B.3], [II.B.4], [III.A.2], [III.A.3], [III.A.4], [III.A.5], [III.A.6], [III.A.7], [III.A.8], [III.A.9] (помечены в таблице цветом) в дальнейшем могут не рассматриваться как маловероятные, так как имеют коэффициент опасности ниже порогового значения δ_i = 0,056.

Перечень актуальных источников угроз ИБ

Код	Источники угроз информационной безопасности	$(k_1)_i$	$(k_2)_i$	$(k_3)_i$	$(K_{on})_i$
[I.A.2]	потенциальные преступники и хакеры	**3**	**3**	**4**	**0,07**
[I.B.1]	основной персонал (пользователи, программисты, разработчики)	**3**	**5**	**4**	**0,13**
[II.A.2]	сети инженерных коммуникации (водоснабжения, канализации)	**4**	**1**	**2**	**0,14**
[II.B.1]	некачественные технические средства обработки информации	**4**	**4**	**5**	**0,10**
[II.B.2]	некачественные программные средства обработки информации	**5**	**5**	**5**	**0,16**
[III.A.1]	пожары	**4**	**5**	**5**	**0,10**

6. Ранжирование групп методов реализации угроз ИБ

Для оценки и ранжирования, по формуле

$$(Kg_m)_N = \frac{Kg_m}{\sum_1 (Kg_m)}$$

рассчитываются нормированные весовые коэффициенты групп методов реализации угроз ИБ $(\mathbf{Kg_m})_{\mathbf{N}}$.

При заполнении таблицы используются следующие формулы

$$Kg_m = \sum (K_A)_k$$

$$(Kg_{mi})_N = \frac{Kg_{mi}}{\sum_1 (Kg_{mi})}$$

$$Kg_{mi} = (Kg_m)_N \times \left[\sum (Kg_i)_N\right]$$

Нормированные весовые коэффициенты групп методов реализации угроз и взаимосвязи групп методов реализации и источников угроз при равенстве приоритетов целей информационной безопасности

gm	Код	Группа методов реализации угроз ИБ	Kg_m	$(Kg_m)_N$	Kg_{mi}	$(Kg_{mi})_N$
1	[M1.A.0]	Активные аналитические методы	**0,33**	**0,06**	**0,029**	**0,06**
2	[M1.B.0]	Пассивные аналитические методы	**0,33**	**0,06**	**0,035**	**0,07**
3	[M2.A.0]	Активные технические методы	**0,77**	**0,15**	**0,081**	**0,16**
4	[M2.B.0]	Пассивные технические методы	**0,22**	**0,04**	**0,023**	**0,05**
5	[M3.A.0]	Активные программно-аппаратные методы	**1,00**	**0,19**	**0,105**	**0,21**
6	[M3.B.0]	Пассивные программно-аппаратные методы	**0,33**	**0,06**	**0,035**	**0,07**
7	[M4.A.0]	Активные социальные методы	**0,93**	**0,18**	**0,098**	**0,20**
8	[M5.A.0]	Активные организационные методы	**0,78**	**0,15**	**0,040**	**0,08**
9	[M6.0.0]	Предпосылки реализации угроз	**0,44**	**0,09**	**0,046**	**0,09**

5. Расчет коэффициента корреляции

Нормированный коэффициент корреляции рассчитывается по формуле

$$(Kg_u)_N = \frac{'(Kg_u)}{\max\{'(Kg_u)\}}$$

Коэффициент корреляции $'(Kg_u)$ рассчитывается по формуле

$$'(Kg_u) = \frac{\max\{g_m\} \times Kg_u}{Qg_u \times \left[\sum_1^{g_u}(Kg_u)\right]}$$

где $\mathbf{Qg_u}$ – число, равное количеству групп методов реализации, использующих группу уязвимостей с индексом $\mathbf{g_u}$.

$\mathbf{max\{g_m\}}$ – максимальное число групп методов реализации, численно $\mathbf{max\{g_m\}}$ = 9.

$$Kg_u = \sum(Kg_{mi})_N$$

Результаты расчета с указанием промежуточных результатов, проведенного в соответствии с методическими рекомендациями сведены в таблицу.

Коэффициенты корреляции и промежуточные результаты расчетов

g_u	Код	Группа методов реализации угроз ИБ	Kg_u	$'(Kg_u)_N$	$(Kg_u)_N$
1	[A.I.0.0]	Сопутствующие излучения	**0,12**	**0,11**	**0,42**
2	[A.II.0.0]	Активизируемые	**0,46**	**0,18**	**0,64**
3	[A.III.0.0]	Особенности элементов	**0,21**	**0,20**	**0,73**
4	[A.IV.0.0]	Особенности объекта	**0,90**	**0,21**	**0,78**
5	[B.I.0.0]	Ошибки (халатность)	**0,48**	**0,23**	**0,83**
6	[B.II.0.0]	Нарушения	**0,90**	**0,21**	**0,78**
7	[B.III.0.0]	Психогенные	**0,54**	**0,26**	**0,94**
8	[C.I.0.0]	Сбои и отказы	**0,38**	**0,24**	**0,88**
9	[C.II.0.0]	Косвенные причины	**0,72**	**0,28**	**1,00**

$(k_1)_f$ – показатель фатальности

$(k_1)_f$ – показатель удобства

$(k_1)_f$ – показатель количества

$$(K_{\text{оп}})_f = \frac{\prod_{n=1}^{3}(k_n)_f}{125} \times (Kg_u)_N$$

Ориентировочная оценка степени опасности уязвимостей

Код	Уязвимости	$(k_1)_f$	$(k_2)_f$	$(k_3)_f$	$(K_{\text{оп}})_f$
[A.I.0.0]	**сопутствующие техническим средствам излучения**	**$(Kg_u)_N$ = 0,42**			
[A.I.a.1]	побочные излучения элементов технических средств	**3**	**4**	**4**	**0,16**
[A.I.a.2]	излучения кабельных линий технических средств	**4**	**3**	**4**	**0,16**
[A.I.a.3]	излучения на частотах работы генераторов	**3**	**4**	**3**	**0,12**
[A.I.a.4]	излучения на частотах самовозбуждения усилителей	**3**	**3**	**3**	**0,09**
[A.I.b.1]	наводки электромагнитных излучений на линии и проводники	**2**	**3**	**3**	**0,06**
[A.I.b.2]	просачивание сигналов в цепи электропитания, в цепи заземления	**2**	**3**	**5**	**0,10**
[A.I.b.3]	неравномерность потребления тока электропитания	**2**	**3**	**5**	**0,10**
[A.I.c.1]	акустические излучения	**2**	**2**	**3**	**0,04**
[A.I.c.2]	виброакустические излучения	**2**	**2**	**3**	**0,04**
[A.II.0.0]	**активизируемые**	**$(Kg_u)_N$ = 0,64**			
[A.II.a.1]	аппаратные закладки устанавливаемые в телефонные линии	**5**	**2**	**3**	**0,15**
[A.II.a.2]	аппаратные закладки устанавливаемые в сети электропитания	**4**	**2**	**3**	**0,12**
[A.II.a.3]	аппаратные закладки устанавливаемые в помещениях	**4**	**3**	**3**	**0,18**
[A.II.a.4]	аппаратные закладки устанавливаемые в технических средствах	**5**	**4**	**5**	**0,51**
[A.II.b.1]	вредоносные программы	**5**	**5**	**5**	**0,64**
[A.II.b.2]	технологические выходы из программ	**3**	**3**	**4**	**0,18**
[A.II.b.3]	нелегальные копии ПО	**3**	**4**	**3**	**0,18**
[A.III.0.0]	**определяемые особенностями элементов**	**$(Kg_u)_N$ = 0,73**			

[A.III.a.1]	обладающие электроакустическими преобразованиями ТА	**2**	**3**	**2**	**0,07**
[A.III.a.2]	обладающие электроакустическими преобразованиями громкоговорители	**2**	**3**	**2**	**0,07**
[A.III.a.3]	обладающие электроакустическими преобразованиями индуктивности	**2**	**3**	**2**	**0,07**
[A.III.a.4]	обладающие электроакустическими преобразованиями дроссели	**2**	**3**	**2**	**0,07**
[A.III.a.5]	обладающие электроакустическими преобразованиями трансформаторы	**2**	**3**	**2**	**0,07**
[A.III.b.1]	подверженные воздействию электромагнитного поля магнитные носители	**5**	**1**	**3**	**0,09**
[A.III.b.2]	подверженные воздействию электромагнитного поля микросхемы	**4**	**1**	**3**	**0,07**
[A.III.b.3]	нелинейные элементы, подверженные ВЧ навязыванию	**2**	**1**	**2**	**0,02**
[A.IV.0.0]	**определяемые особенностями защищаемого объекта**	**$(Kg_u)_N$ = 0,78**			
[A.IV.a.1]	отсутствие контролируемой зоны	**4**	**5**	**4**	**0,50**
[A.IV.a.2]	наличие прямой видимости объектов	**4**	**4**	**4**	**0,40**
[A.IV.a.3]	наличие удаленных и мобильных элементов объекта	**3**	**3**	**4**	**0,18**
[A.IV.a.4]	наличие вибрирующих отражающих поверхностей	**2**	**3**	**3**	**0,11**
[A.IV.b.1]	использование радиоканалов	**2**	**2**	**3**	**0,07**
[A.IV.b.2]	использование глобальных информационных сетей	**5**	**5**	**5**	**0,78**
[A.IV.b.3]	использование арендуемых каналов	**3**	**5**	**4**	**0,37**
[B.I.0.0]	**ошибки (халатность)**	**$(Kg_u)_N$ = 0,83**			
[B.I.a.1]	ошибки при разработке алгоритмов и программного обеспечения	**3**	**3**	**3**	**0,18**
[B.I.a.2]	ошибки при инсталляции и загрузке программного обеспечения	**3**	**4**	**5**	**0,39**
[B.I.a.3]	ошибки при эксплуатации программного обеспечения	**4**	**5**	**5**	**0,66**
[B.I.a.4]	ошибки при вводе данных (информации)	**2**	**3**	**4**	**0,16**
[B.I.a.5]	ошибки при настройке сервисов универсальных систем	**2**	**3**	**3**	**0,12**
[B.I.a.6]	ошибки самообучающейся сложной системы систем	**1**	**5**	**1**	**0,03**
[B.I.b.1]	ошибки при включении/выключении технических средств	**3**	**5**	**5**	**0,50**

[B.I.b.2]	ошибки при использовании технических средств охраны	**2**	**3**	**3**	**0,12**
[B.I.b.3]	ошибки при использовании средств обмена информацией	**3**	**4**	**3**	**0,23**
[B.I.c.1]	ошибки при конфигурировании и управлении сложной системы	**2**	**3**	**2**	**0,08**
[B.I.c.2]	ошибки при настройке программного обеспечения	**3**	**3**	**3**	**0,18**
[B.I.c.3]	ошибки при организации управления потоками обмена информации	**3**	**4**	**3**	**0,23**
[B.I.c.4]	ошибки при настройке технических средств	**3**	**3**	**3**	**0,18**
[B.I.c.5]	ошибки при настройке штатных средств защиты ПО	**3**	**2**	**3**	**0,12**
[B.I.d.1]	повреждение (удаление) программного обеспечения	**3**	**3**	**3**	**0,18**
[B.I.d.2]	повреждение (удаление) данных	**5**	**5**	**5**	**0,83**
[B.I.d.3]	повреждение (уничтожение) носителей информации	**5**	**4**	**4**	**0,53**
[B.I.d.4]	повреждение каналов связи	**3**	**3**	**3**	**0,18**
[B.II.0.0]	**нарушения**	**$(Kg_u)_N$ = 0,78**			
[B.II.a.1]	нарушения доступа на объект	**3**	**3**	**2**	**0,11**
[B.II.a.2]	нарушения доступа к техническим средствам	**5**	**4**	**5**	**0,62**
[B.II.a.3]	нарушения соблюдения конфиденциальности	**4**	**4**	**4**	**0,39**
[B.II.b.1]	нарушения энергообеспечения	**3**	**3**	**3**	**0,17**
[B.II.b.2]	нарушения жизнеобеспечения	**2**	**4**	**4**	**0,20**
[B.II.b.3]	установка нештатного оборудования	**4**	**3**	**2**	**0,15**
[B.II.b.4]	инсталляция нештатного ПО (игрового, обучающего и др.)	**2**	**3**	**3**	**0,11**
[B.II.c.1]	нарушения режима обработки и обмена информацией	**3**	**3**	**3**	**0,17**
[B.II.c.2]	нарушения режима хранения и уничтожения носителей информации	**3**	**3**	**3**	**0,62**
[B.II.c.3]	нарушения режима уничтожения производственных отходов и брака	**2**	**3**	**3**	**0,28**
[B.III.0.0]	**психогенные**	**$(Kg_u)_N$ = 0,94**			
[B.III.a.1]	антагонистические отношения (зависть, озлобленность, обида)	**3**	**2**	**2**	**0.09**
[B.III.a.3]	неудовлетворенность своим положением	**3**	**3**	**2**	**0,14**
[B.III.a.4]	неудовлетворенность действиями руководства	**3**	**3**	**2**	**0,14**

[B.III.a.5]	психологическая несовместимость	**2**	**3**	**2**	**0,09**
[B.III.b.1]	психические отклонения	**2**	**3**	**2**	**0,09**
[B.III.b.2]	стрессовые ситуации	**3**	**4**	**2**	**0,18**
[C.I.0.0]	**сбои и отказы**	**$(Kg_u)_N$ = 0,88**			
[C.I.a.1]	отказы ТС обрабатывающих информацию	**3**	**3**	**3**	**0,19**
[C.I.a.2]	отказы ТС обеспечивающих работоспособность средств обработки	**3**	**3**	**3**	**0,19**
[C.I.a.3]	отказы ТС обеспечивающих охрану и контроль доступа	**3**	**4**	**2**	**0,17**
[C.I.b.1]	старение и размагничивание дискет и съемных носителей	**3**	**2**	**3**	**0,13**
[C.I.b.2]	старение и размагничивание жестких дисков	**3**	**4**	**2**	**0,17**
[C.I.b.3]	старение элементов микросхем	**2**	**4**	**3**	**0,17**
[C.I.b.4]	старение кабелей и соединительных линий	**2**	**4**	**3**	**0,17**
[C.I.c.1]	сбои операционных систем и СУБД	**4**	**5**	**4**	**0,56**
[C.I.c.2]	сбои прикладных программ	**3**	**3**	**3**	**0,19**
[C.I.c.3]	сбои сервисных программ	**2**	**3**	**3**	**0,13**
[C.I.c.4]	сбои антивирусных программ	**4**	**4**	**4**	**0,45**
[C.I.d.1]	сбои электропитания оборудования, обрабатывающего информацию	**3**	**3**	**3**	**0,19**
[C.I.d.2]	сбои электропитания обеспечивающего и вспомогательного оборудования	**3**	**3**	**3**	**0,19**
[C.II.0.0]	**косвенные причины**	**$(Kg_u)_N$ = 1,00**			
[C.II.a.1]	критично близкое расположение техногенных сооружений	**3**	**5**	**1**	**0,12**
[C.II.a.2]	географическое положение объекта и климатические условия	**1**	**5**	**1**	**0,04**
[C.II.a.3]	гидрологическая и сейсмологическая обстановка	**1**	**5**	**1**	**0,04**
[C.II.b.1]	физический износ оборудования и сооружений	**4**	**5**	**1**	**0,16**
[C.II.b.2]	малое время наработки на отказ оборудования и ПО	**4**	**5**	**1**	**0,16**
[C.II.b.3]	повреждения жизнеобеспечивающих коммуникаций	**4**	**3**	**2**	**0,19**
[C.II.c.1]	физическое состояние субъекта	**3**	**4**	**2**	**0,19**
[C.II.c.2]	психосоматическое состояние субъекта	**4**	**3**	**2**	**0,19**

$$\delta_u = 0{,}2 \times \max\{(Kg_u)_N\} = 0{,}20$$

Уязвимости [A.I.a.1], [A.I.a.2], [A.I.a.3], [A.I.a.4], [A.I.b.1], [A.I.b.2], [A.I.b.3], [A.I.c.1], [A.I.c.2], [A.II.a.1], [A.II.a.2], [A.II.a.3], [A.II.b.2] ,[A.II.b.3], [A.III.a.1], [A.III.a.2], [A.III.a.3], [A.III.a.4], [A.III.a.5], [A.III.b.1], [A.III.b.2], [A.III.b.3], [A.IV.a.3], [A.IV.a.4], [A.IV.b.1], [B.I.a.1], [B.I.a.4], [B.I.a.5], [B.I.a.6], [B.I.b.2], [B.I.c.1], [B.I.c.2], [B.I.c.4], [B.I.c.5], [B.I.d.1], [B.I.d.4], [B.II.a.1], [B.II.b.1], [B.II.b.2], [B.II.b.3], [B.II.b.4], [B.II.c.1], [B.II.c.2], [B.II.c.3], [B.III.a.1], [B.III.a.3], [B.III.a.4], [B.III.a.5], [B.III.b.1], [B.III.b.2], [C.I.a.1], [C.I.a.2], [C.I.a.3], [C.I.b.1], [C.I.b.2], [C.I.b.3], [C.I.b.4], [C.I.c.2], [C.I.c.3], [C.I.d.1], [C.I.d.2], [C.II.a.1], [C.II.a.2], [C.II.a.3], [C.II.b.1], [C.II.b.2], [C.II.b.3], [C.II.c.1], [C.II.c.2], помеченные в таблице цветом, в дальнейшем могут не рассматриваться как маловероятные, так как имеют коэффициент опасности ниже порогового значения δ_f = 0,20.

Перечень актуальных уязвимостей

Код	Уязвимости	$(k_1)_f$	$(k_2)_f$	$(k_3)_f$	$(K_{оп})_f$
[A.II.a.4]	аппаратные закладки, устанавливаемые в технических средствах	**5**	**4**	**5**	**0,51**
[A.II.b.1]	вредоносные программы	**5**	**5**	**5**	**0,64**
[A.IV.a.1]	отсутствие контролируемой зоны	**4**	**5**	**4**	**0,50**
[A.IV.a.2]	наличие прямой видимости объектов	**4**	**4**	**4**	**0,40**
[A.IV.b.2]	использование глобальных информационных сетей	**5**	**5**	**5**	**0,78**
[A.IV.b.3]	использование арендуемых каналов	**3**	**5**	**4**	**0,37**
[B.I.a.2]	ошибки при инсталляции и загрузке программного обеспечения	**3**	**4**	**5**	**0,39**
[B.I.a.3]	ошибки при эксплуатации программного обеспечения	**4**	**5**	**5**	**0,66**
[B.I.b.1]	ошибки при включении/выключении технических средств	**3**	**5**	**5**	**0,50**
[B.I.b.3]	ошибки при использовании средств обмена информацией	**3**	**4**	**3**	**0,23**
[B.I.c.3]	ошибки при организации управления потоками обмена информации	**3**	**4**	**3**	**0,23**
[B.I.d.2]	повреждение (удаление) данных	**5**	**5**	**5**	**0,83**
[B.I.d.3]	повреждение (уничтожение) носителей информации	**5**	**4**	**4**	**0,53**
[B.II.a.2]	нарушения доступа к техническим средствам	**5**	**4**	**5**	**0,62**
[B.II.a.3]	нарушения соблюдения конфиденциальности	**4**	**4**	**4**	**0,39**
[C.I.c.1]	сбои операционных систем и СУБД	**4**	**5**	**4**	**0,56**
[C.I.c.4]	сбои антивирусных программ	**4**	**4**	**4**	**0,45**

Перечень актуальных угроз

k	Угрозы ИБ	$(К_А)_k$
1	Хищение (копирование) информации и средств ее обработки	**0,22**
2	Уничтожение информации и средств ее обработки	**0,2**
3	Блокирование информации	**0,13**

ВОЗМОЖНЫЕ ВАРИАНТЫ АТАК

I. Реализация угрозы «ХИЩЕНИЕ»

[I.B.1]	[M2.A.01]	[B.II.a.2]
[I.B.2]	[M2.B.03]	[B.I.b.3]

II. Реализация угроз «БЛОКИРОВАНИЕ» и «УНИЧТОЖЕНИЕ»

[I.A.2]	[M3.B.02]	[B.II.a.2]
[I.B.1]	[M5.A.01]	[B.II.a.2]
[I.B.2]	[M3.B.02]	[A.II.b.1]
[I.B.2]	[M3.B.02]	[B.I.d.2]