ГУАП

Кафедра № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

Профессор, д.т.н.		Н.Н. Мошак
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ПРАКТИЧЕСКАЯ РАБОТА №1

Оценка риска информационной безопасности корпоративной информационной системы на основе модели угроз и уязвимостей

по курсу: БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 3931		К.В. Жук
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2022

Цель работы:

Рассчитать риск информационной безопасности корпоративной информационной системы на основе модели угроз и уязвимостей.

Теоретические положения:

Расчет рисков по угрозе информационной безопасности

На **первом этапе** рассчитывается уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$\mathrm{Th_{c,I,a}} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $\mathrm{ER_{c,I,a}}$ – *критичность реализации угрозы* (указывается в %);

$\mathrm{P(V)_{c,I,a}}$ – *вероятность реализации угрозы через данную уязвимость* (указывается в %).

Вычисляется одно или три значения в зависимости от количества базовых угроз. Получается значение *уровня угрозы по уязвимости* в интервале от 0 до 1.

Для расчета уровня угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе, суммируются полученные уровни угроз через конкретные уязвимости по следующей формуле:

Для режима с одной базовой угрозой:

$$\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$$

Для режима с тремя базовыми угрозами:

$$\mathrm{CTh_c} = 1 - \prod_{i=1}^{n} (1 - Th_c)$$

$$\mathrm{CTh_i} = 1 - \prod_{i=1}^{n} (1 - Th_i)$$

$$\mathrm{CTh_a} = 1 - \prod_{i=1}^{n} (1 - Th_a)$$

Значения *уровня угрозы по всем уязвимостям* получаются в интервале от 0 до 1.

Аналогично рассчитывается общий уровень угроз по ресурсу CThR (учитывая все угрозы, действующие на ресурс):

Для режима с одной базовой угрозой:

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh)$$

Для режима с тремя базовыми угрозами:

$$\mathrm{CThR_c} = 1 - \prod_{i=1}^{n} (1 - CTh_c)$$

$$\mathrm{CThR_i} = 1 - \prod_{i=1}^{n} (1 - CTh_i)$$

$$\mathrm{CThR_a} = 1 - \prod_{i=1}^{n} (1 - CTh_a)$$

Значение *общего уровня угрозы* получается в интервале от 0 до 1.

Риск по ресурсу R рассчитывается следующим образом:

Для режима с одной базовой угрозой:

$$\mathrm{R} = CThR \times D,$$

где D – критичность ресурса. Задается в деньгах или уровнях.

В случае угрозы доступность (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:

$$D_{a/год} = D_{a/час} \times T$$

Для остальных угроз критичность ресурса задается в год. Для режима с тремя базовыми угрозами:

$$\mathrm{R_c} = CThR_c \times D_c$$

$$\mathrm{R_i} = CThR_i \times D_i$$

$$\mathrm{R_a} = CThR_a \times D_a$$

$$\mathrm{R} = (1 - \prod_{i=1}^{3} (1 - \frac{R_i}{100})) \times 100$$

$\mathrm{D_{a,c,i}}$ – критичность ресурса по трем угрозам. Задается в деньгах или уровнях.

R - суммарный риск по трем угрозам.

Таким образом, получается значение ***риска по ресурсу*** в уровнях (заданных пользователем) или деньгах.

Риск по информационной системе CR рассчитывается по формуле:

Для режима с одной базовой угрозой:

1) Для режима работы в деньгах:

$$CR = \sum_{i=1}^{n} R_i$$

2) Для режима работы в уровнях:

$$\mathrm{CR} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100$$

Для режима работы с тремя угрозами:

1) Для режима работы в деньгах:

$$CR_{a,c,i} = \sum_{i=1}^{n} R_i$$

$$CR = \sum_{i=1}^{n} CR_{a,c,i}$$

$\mathrm{CR_{a,c,I}}$ - риск по системе по каждому виду угроз

CR - риск по системе суммарно по трем видам угроз

2) Для режима работы в уровнях:

$$\mathrm{CR_{a,c,i}} = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100$$

$$\mathrm{CR} = (1 - \prod_{i=1}^{3}(1 - \frac{R_{a,c,i}}{100})) \times 100$$

Задание контрмер

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. Т.е. на выходе пользователь получает значение двух рисков – риска без учета контрмеры **(Rold**) и риск с учетом заданной контрмеры **(Rnew**) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры рассчитывается по следующей формуле (**E**):

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результате работы алгоритма пользователь системы получает следующие данные:

• Риск по трем базовым угрозам (или по одной суммарной угрозе) *для ресурса;*

• Риск суммарно по всем угрозам *для ресурса*;

• Риск по трем базовым угрозам (или по одной суммарной угрозе) *для информационной системы;*

• Риск по всем угрозам для *информационной системы;*

• Риск по всем угрозам для информационной системы *после задания контрмер;*

• Эффективность контрмеры;

• Эффективность комплекса контрмер.

Ход выполнения работы:

Обобщенная схема

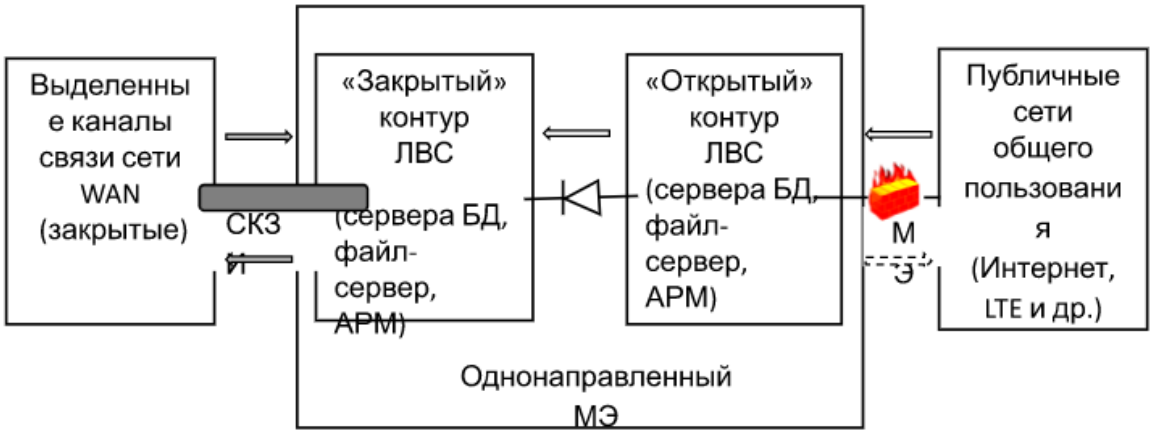

Рис.1 – Обобщенная схема информационных потоков в ИС

Модель угроз и уязвимостей

Таблица 1

Ресурс	*Угрозы*	*Уязвимости*
1.Сервер закрытого контура (критичность ресурса 120 у.е)	1.Неавторизованное проникновение нарушителя внутрь охраняемого периметра	1.Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
		2. Отсутствие системы видеонаблюдения
	2.Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе	1.Отсутствие авторизации для внесения изменений в систему электронной почты
		2.Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции

	3. Разглашение конфиденциальной информации сотрудниками организации	1.Отсутствие соглашений о конфиденциальности
		2. Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками
2.Сервер открытого контура (критичность ресурса 100 у.е)	1. Угроза некорректного использования функционала программного и аппаратного обеспечения	1. Отсутствие настроек авторизации пользователей
		2. Слабая система хранения паролей
	2.Угроза доступа неавторизированных пользователей к файловой системе	1. Отсутствие настроек авторизации пользователей
		2.Слабая технология защиты файловой системы
	3. Угроза длительного удержания вычислительных ресурсов пользователями	1.Слабый механизм балансировки нагрузки
		2. Отсутствие настроек авторизации пользователей
3.МЭ открытого контура (критичность ресурса 65 у.е)	1. Отказ в обслуживании	1.Отсутствиерезервного межсетевого экрана
		2.Низкая пропускная способность межсетевого экрана
	2. Разглашение текущей конфигурации устройства	1. Отсутствие соглашений о конфиденциальности
		2. Отсутствие системы аутентификации
	3 Неавторизованный доступ к настройке МЭ	1. Отсутствие настроек авторизации пользователей
		2. Использование устаревших алгоритмов аутентификации для хранения паролей
4.СКЗИ закрытого контура (критичность ресурса 60 у.е)	1.Отказ в обслуживании	1.Отсутствиемежсетевого экрана
		2. Отсутствие аутентификации при подключении к зашифрованному каналу
	2.Угроза анализа криптографических алгоритмов и их реализации	1. Использование слабых криптографических алгоритмов
		2.Наличие ошибок в программном коде криптографических средств

	3.Неограниченный доступ нарушителя к информации	1.Использование слабых или устаревших криптографических алгоритмов
		2. Отсутствие соглашения о конфиденциальности
5. Однонаправленный шлюз (критичность ресурса 80 у.е)	1.Отказ в обслуживании	1.Отсутствие резервный межсетевой экран
		2.Низкая пропускная способность шлюза
	2.Реализацияатаки «Man in the Middle» путем возможного подключения к закрытому каналу	1. Отсутствие криптографических средств, применяемых к передаваемой информации
		2.Отсутствие контроля доступа к закрытому каналу
	3.Угроза перехвата привилегированного потока	1. Наличие ошибок в программном коде криптографических средств
		2. Отсутствие аутентификации при подключении к закрытому каналу
6. Оборудование ЛВС открытого контура (критичность ресурса 80 у.е)	1. Перехват передаваемых сообщений	1.Неправильная конфигурация средств криптографических средств защиты информации
		2.Использование алгоритмов шифрования с недостаточной длиной ключа
	2.Модификация и удаление передаваемых сообщений	1. Отсутствие алгоритмов аутентификации
		2. Использование устаревшего алгоритма аутентификации
	3.Прослушивание привилегированного трафика	1.Отсутствие криптографической защиты, применяемой к пакетам данных
		2.Отсутствие контроля доступа к защищенному каналу
7. Оборудование ЛВС закрытого контура (критичность ресурса 95 у.е)	1. Прослушивание привилегированного трафика	1. Отсутствие криптографической защиты, применяемой к пакетам данных
		2. Отсутствие контроля доступа к защищенному каналу
	2.Модификация и удаление передаваемых сообщений	1. Отсутствие алгоритмов аутентификации
		2. Использование устаревшего алгоритма аутентификации
	3.Перехват передаваемых сообщений	1. Неправильная конфигурация средств криптографических средств защиты информации
		2. Отсутствие регламента смены пароля

Расчет вероятности и критичности для каждой угрозы для аппаратных ресурсов

Таблица 2

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через уязвимость (%), ER
Сервер закрытого контура		
Угроза1/Уязвимость 1	85	80
Угроза1/Уязвимость 2	70	45
Угроза2/Уязвимость 1	70	50
Угроза2/Уязвимость 2	75	65
Угроза3/Уязвимость 1	65	25
Угроза3/Уязвимость 2	50	30
Сервер открытого контура		
Угроза1/Уязвимость 1	45	55
Угроза1/Уязвимость 2	75	65
Угроза2/Уязвимость 1	25	30
Угроза2/Уязвимость 2	25	15
Угроза3/Уязвимость 1	60	45
Угроза3/Уязвимость 2	55	15
МЭ открытого контура		
Угроза1/Уязвимость 1	85	25
Угроза1/Уязвимость 2	55	55
Угроза2/Уязвимость 1	75	50
Угроза2/Уязвимость 2	50	60
Угроза3/Уязвимость 1	35	30
Угроза3/Уязвимость 2	50	60
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	30	20
Угроза1/Уязвимость 2	90	70

Угроза2/Уязвимость 1	25	15
Угроза2/Уязвимость 2	45	25
Угроза3/Уязвимость 1	20	35
Угроза3/Уязвимость 2	60	50
Однонаправленный шлюз		
Угроза1/Уязвимость 1	75	60
Угроза1/Уязвимость 2	80	55
Угроза2/Уязвимость 1	45	35
Угроза2/Уязвимость 2	55	30
Угроза3/Уязвимость 1	50	30
Угроза3/Уязвимость 2	40	30
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	25	35
Угроза1/Уязвимость 2	65	40
Угроза2/Уязвимость 1	60	50
Угроза2/Уязвимость 2	45	15
Угроза3/Уязвимость 1	10	20
Угроза3/Уязвимость 2	55	20
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	75	45
Угроза1/Уязвимость 2	50	30
Угроза2/Уязвимость 1	80	70
Угроза2/Уязвимость 2	85	75
Угроза3/Уязвимость 1	55	40
Угроза3/Уязвимость 2	60	40

Расчёт уровня угрозы по уязвимости Th и уровня угрозы по всем уязвимостям, через которые реализуется данная угроза CTh

Таблица 3

Угроза/Уязвимость	Уровень угрозы Th $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,68	0,781
Угроза1/Уязвимость 2	0,315	
Угроза2/Уязвимость 1	0,35	0,667
Угроза2/Уязвимость 2	0,4875	
Угроза3/Уязвимость 1	0,1625	0,288
Угроза3/Уязвимость 2	0,15	
Сервер открытого контура		
Угроза1/Уязвимость 1	0,2475	0,614
Угроза1/Уязвимость 2	0,4875	
Угроза2/Уязвимость 1	0,075	0,11
Угроза2/Уязвимость 2	0,0375	
Угроза3/Уязвимость 1	0,27	0,33
Угроза3/Уязвимость 2	0,0825	
МЭ открытого контура		
Угроза1/Уязвимость 1	0,2125	0,45
Угроза1/Уязвимость 2	0,3025	
Угроза2/Уязвимость 1	0,375	0,563
Угроза2/Уязвимость 2	0,3	
Угроза3/Уязвимость 1	0,105	0,374

Угроза3/Уязвимость 2	0,3	
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,06	0,652
Угроза1/Уязвимость 2	0,63	
Угроза2/Уязвимость 1	0,0375	0,146
Угроза2/Уязвимость 2	0,1125	
Угроза3/Уязвимость 1	0,07	0,349
Угроза3/Уязвимость 2	0,3	
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,45	0,692
Угроза1/Уязвимость 2	0,44	
Угроза2/Уязвимость 1	0,1575	0,296
Угроза2/Уязвимость 2	0,165	
Угроза3/Уязвимость 1	0,15	0,252
Угроза3/Уязвимость 2	0,12	
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,0875	0,325
Угроза1/Уязвимость 2	0,26	
Угроза2/Уязвимость 1	0,3	0,347
Угроза2/Уязвимость 2	0,0675	
Угроза3/Уязвимость 1	0,02	0,1278
Угроза3/Уязвимость 2	0,11	
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,3375	0,437
Угроза1/Уязвимость 2	0,15	
Угроза2/Уязвимость 1	0,56	0,871
Угроза2/Уязвимость 2	0,6375	

Угроза3/Уязвимость 1	0,22	0,407
Угроза3/Уязвимость 2	0,24	

Расчет общего уровня угроз, действующих на ресурс, а также вычислим риск каждого ресурса

Таблица 4

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), CThR $\mathrm{CThR} = 1 - \prod_{i=1}^{n}(1 - CTh)$	Риск ресурса для режима с одной общей угрозой (%), R $\mathrm{R} = CThR \times D$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,95	0,95 * 120 = 114
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Сервер открытого контура		
Угроза1/Уязвимость 1	0,77	0,77 * 100 = 77
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
МЭ открытого контура		
Угроза1/Уязвимость 1	0,849	0,849 * 65 = 55,185
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		

Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,806	0,806 * 60 = 48,36
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,837	0,837 * 80 = 66,96
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,615	0,615 * 80 = 49,2
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,956	0,956 * 95 = 90,82
Угроза1/Уязвимость 2		

Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		

Контрмеры

Контрмеры необходимы для того, чтобы понизить вероятность эксплуатации угроз через их уязвимости. Возьмем **15%** как максимально допустимую вероятность компрометации системы.

- Ввести систему видеонаблюдения в серверных;
- Составить соглашение о конфиденциальности для сотрудников;
- Ввести ролевую систему доступа на сервере;
- Установить резервный межсетевой экран в открытой зоне;
- Настроить аутентификацию при удаленном и консольном подключении ко всем устройствам;
- Поставить межсетевой экран на защищенный канал;
- Настроить аутентификацию при подключении к зашифрованному каналу;
- Повысить пропускную способность шлюза;
- Настроить более современные алгоритмы шифрования;
- Увеличить длину ключей шифрования.

Расчет вероятности реализации угрозы с учетом контрмер

Таблица 5

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%),P(V)	Критичность реализации угрозы через уязвимость (%),ER
Сервер закрытого контура		
Угроза1/Уязвимость 1	3	80
Угроза1/Уязвимость 2	7	45
Угроза2/Уязвимость 1	5	50
Угроза2/Уязвимость 2	4	65
Угроза3/Уязвимость 1	6	30
Угроза3/Уязвимость 2	5	30

Сервер открытого контура		
Угроза1/Уязвимость 1	8	55
Угроза1/Уязвимость 2	5	65
Угроза2/Уязвимость 1	7	30
Угроза2/Уязвимость 2	11	15
Угроза3/Уязвимость 1	5	45
Угроза3/Уязвимость 2	7	15
МЭ открытого контура		
Угроза1/Уязвимость 1	10	25
Угроза1/Уязвимость 2	8	55
Угроза2/Уязвимость 1	7	50
Угроза2/Уязвимость 2	4	60
Угроза3/Уязвимость 1	5	30
Угроза3/Уязвимость 2	5	60
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	7	20
Угроза1/Уязвимость 2	5	70
Угроза2/Уязвимость 1	10	15
Угроза2/Уязвимость 2	5	25
Угроза3/Уязвимость 1	5	35
Угроза3/Уязвимость 2	6	50
Однонаправленный шлюз		
Угроза1/Уязвимость 1	7	60
Угроза1/Уязвимость 2	9	55
Угроза2/Уязвимость 1	5	35
Угроза2/Уязвимость 2	3	30
Угроза3/Уязвимость 1	5	30

Угроза3/Уязвимость 2	3	30
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	5	35
Угроза1/Уязвимость 2	9	40
Угроза2/Уязвимость 1	6	50
Угроза2/Уязвимость 2	10	15
Угроза3/Уязвимость 1	5	20
Угроза3/Уязвимость 2	5	20
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	8	45
Угроза1/Уязвимость 2	10	30
Угроза2/Уязвимость 1	5	70
Угроза2/Уязвимость 2	5	75
Угроза3/Уязвимость 1	3	40
Угроза3/Уязвимость 2	4	40

Расчёт уровня угрозы по уязвимости Th и уровня угрозы по всем уязвимостям, через которые реализуется данная угроза CTh с учетом контрмер

Таблица 6

Угроза/Уязвимость	Уровень угрозы (%),Th $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%),CTh $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,024	0,045
Угроза1/Уязвимость 2	0,031	
Угроза2/Уязвимость 1	0,025	0,05
Угроза2/Уязвимость 2	0,026	

Угроза3/Уязвимость 1	0,018	0,032
Угроза3/Уязвимость 2	0,015	
Сервер открытого контура		
Угроза1/Уязвимость 1	0,044	0,07
Угроза1/Уязвимость 2	0,0325	
Угроза2/Уязвимость 1	0,021	0,037
Угроза2/Уязвимость 2	0,0165	
Угроза3/Уязвимость 1	0,0225	0,032
Угроза3/Уязвимость 2	0,0105	
МЭ открытого контура		
Угроза1/Уязвимость 1	0,025	0,0679
Угроза1/Уязвимость 2	0,044	
Угроза2/Уязвимость 1	0,035	0,058
Угроза2/Уязвимость 2	0,024	
Угроза3/Уязвимость 1	0,015	0,044
Угроза3/Уязвимость 2	0,03	
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,014	0,048
Угроза1/Уязвимость 2	0,035	
Угроза2/Уязвимость 1	0,015	0,027
Угроза2/Уязвимость 2	0,0125	
Угроза3/Уязвимость 1	0,0175	0,046
Угроза3/Уязвимость 2	0,03	
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,042	0,08
Угроза1/Уязвимость 2	0,0495	
Угроза2/Уязвимость 1	0,0175	0,026

Угроза2/Уязвимость 2	0,009	
Угроза3/Уязвимость 1	0,015	0,0238
Угроза3/Уязвимость 2	0,009	
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,0175	0,052
Угроза1/Уязвимость 2	0,036	
Угроза2/Уязвимость 1	0,03	0,044
Угроза2/Уязвимость 2	0,015	
Угроза3/Уязвимость 1	0,01	0,02
Угроза3/Уязвимость 2	0,01	
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,036	0,064
Угроза1/Уязвимость 2	0,03	
Угроза2/Уязвимость 1	0,035	0,071
Угроза2/Уязвимость 2	0,0375	
Угроза3/Уязвимость 1	0,012	0,027
Угроза3/Уязвимость 2	0,016	

Расчет общего уровня угроз, действующих на ресурс и риск ресурса для режима с одной общей угрозой с учетом контрмер

Таблица 7

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%),CThR $\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh)$	Риск ресурса для режима с одной общей угрозой (%), R $\mathrm{R} = CThR \times D$
Сервер закрытого контура		
Угроза1/Уязвимость 1	0,12	14.4
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		

Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Сервер открытого контура		
Угроза1/Уязвимость 1	0,133	13,3
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
МЭ открытого контура		
Угроза1/Уязвимость 1	0,16	10,4
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
СКЗИ закрытого контура		
Угроза1/Уязвимость 1	0,116	6,96
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Однонаправленный шлюз		
Угроза1/Уязвимость 1	0,125	10

Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Оборудование ЛВС открытого контура		
Угроза1/Уязвимость 1	0,111	8,88
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		
Оборудование ЛВС закрытого контура		
Угроза1/Уязвимость 1	0,153	14,53
Угроза1/Уязвимость 2		
Угроза2/Уязвимость 1		
Угроза2/Уязвимость 2		
Угроза3/Уязвимость 1		
Угроза3/Уязвимость 2		

Как видно из таблицы, риски по каждому ресурсу не превышают порога в 15%, следовательно, контрмеры принесли нужный эффект. Если значения были бы выше границы, то пришлось бы вводить дополнительные контрмеры и считать заново.

Расчет эффективности введения контрмер

Таблица 8

Ресурс	$E = \frac{R_{old} - R_{new}}{R_{old}}$
Сервер закрытого контура	0.873
Сервер открытого контура	0.827
МЭ открытого контура	0.811
СКЗИ закрытого контура	0.856
Однонаправленный шлюз	0.850
Оборудование ЛВС открытого контура	0.819
Оборудование ЛВС закрытого контура	0.840

Вывод:

Благодаря этим расчетам специалист по защите информации может примерно оценить риски ресурсов, учесть вероятность появления той или иной угрозы. С помощью этих данных можно провести профилактическую работу по отношению ко всем ресурсам, чтобы максимально обезопасить всю систему от атак или непредумышленных действий пользователей, которые могут привести к потере или искажению важной информации, или привести части системы в негодность. Необходимо понимать важность таких расчетов, потому что каждая минута простоя системы из-за различных угроз, может понести большие убытки для компании.