Цель работы: рассчитать риск информационной безопасности корпоративной информационной системы на основе модели угроз и уязвимостей.

Теоретические положения

1.1 Анализ рисков ИС

Целью анализа рисков является оценка угроз и уязвимостей, возможного ущерба, учитывая уровень защищенности информационной системы. Анализ рисков — это то, с чего должно начинаться построение политики информационной безопасности (ИБ) ИС [9-11]. Он включает в себя мероприятия по обследованию безопасности ИС, целью которых является определение того, какие активы ИС и от каких угроз надо защищать, а также, в какой степени те или иные активы нуждаются в защите [10-21]. В процессе анализа рисков проводятся следующие работы:

– идентификация и определение ценности всех активов в рамках выбранной области деятельности;

– идентификация угроз и уязвимостей для идентифицированных активов;

– оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;

– выбор критериев принятия рисков;

– подготовка плана обработки рисков.

1.2 Основные понятия и допущения модели

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза – действие, которое потенциально может привести к нарушению безопасности.

Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Критичность ресурса (D) – ущерб, который понесет компания от потери ресурса. Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100 или в деньгах.

Критичность реализации угрозы (ER) – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах.

Вероятность реализации угрозы через данную уязвимость в течение года (P(V)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

Максимальное критичное время простоя (T_{max}) - значение времени максимального простоя, которое является критичным для организации. Т.е. ущерб, нанесенный организации при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный организации, не увеличивается.

Структурная схема «закрытого» и «открытого» контура ИС

Современные ИС предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищенности, обрабатывается конфиденциальная информация с различным грифом секретности, а в «открытом» контуре - открытая информация.

Обобщенная схема информационных потоков в ИС:

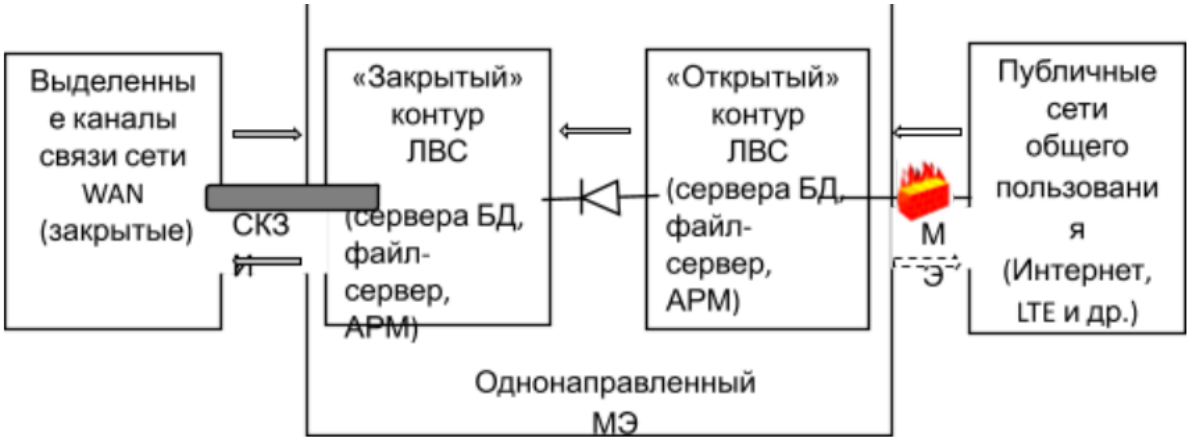

Рисунок 1 - Обобщенная схема информационных потоков

Идентификация активов, определяющих функциональность ИС

- аппаратные ресурсы «закрытого» (сервер БД, СКЗИ, однонаправленный МЭ, оборудование ЛВС, АРМ пользователей) контура и «открытого» контура (сервер БД, Proxy-сервер, внешний МЭ, оборудование ЛВС, АРМ пользователей);
- информационные ресурсы «закрытого» и «открытого» контура (БД);
- программные ресурсы «закрытого» и «открытого» контура (ОС, СУБД, прикладное ПО);
- людские ресурсы;
- имидж организации.

Построение модели угроз и уязвимостей для ИС

Уровень приемлемого риска («остаточный риск») принимаем равным 10% от предполагаемого ущерба по ресурсу.

4.1 Аппаратные ресурсы

Таблица 1 - Модель угроз для аппаратных ресурсов

Ресурс	Критичность ресурса	Угрозы	Уязвимости
Сервер закрытого контура	100 у.е.	Неавторизованное проникновение нарушителя внутрь охраняемого периметра	1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию

			2 Отсутствие системы видеонаблюдения
		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
		Разглашение конфиденциальной информации сотрудниками организации	1 Отсутствие соглашений о конфиденциальности
			2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками
Сервер открытого контура	120 у.е.	Угроза некорректного использования функционала программного и аппаратного обеспечения	1 Отсутствие настроек авторизации пользователей
			2 Слабая система хранения паролей
		Угроза доступа неавторизированных пользователей к файловой системе	1 Отсутствие настроек авторизации пользователей
			2 Слабая технология защиты файловой системы

		Угроза длительного удержания вычислительных ресурсов пользователями	1 Слабый механизм балансировки нагрузки
			2 Отсутствие настроек авторизации пользователей
МЭ открытого контура	80 у.е.	Отказ в обслуживании	1 Отсутствие резервного межсетевого экрана
			2 Низкая пропускная способность межсетевого экрана
		Разглашение текущей конфигурации устройства	1 Разглашение текущей конфигурации устройства
			2 Отсутствие системы аутентификации
		Неавторизованный доступ к настройке МЭ	1 Отсутствие настроек авторизации пользователей
			2 Использование устаревших алгоритмов аутентификации для хранения паролей
СКЗИ закрытого контура	50 у.е.	Отказ в обслуживании	1 Отсутствие межсетевого экрана
			2 Отсутствие аутентификации при подключении к зашифрованному каналу
		Угроза анализа криптографических алгоритмов и их реализации	1 Использование слабых криптографических алгоритмов

			2 Наличие ошибок в программном коде криптографических средств
		Неограниченный доступ нарушителя к информации	1 Использование слабых или устаревших криптографических алгоритмов
			2 Отсутствие соглашения о конфиденциальности
Однонаправленный МЭ	73 у.е.	Отказ в обслуживании	1 Отсутствие резервный межсетевой экран
			2 Низкая пропускная способность шлюза
		Реализация атаки «ManintheMiddle» путем возможного подключения к закрытому каналу	1 Отсутствие криптографических средств, применяемых к передаваемой информации
			2 Отсутствие контроля доступа к закрытому каналу
		Угроза перехвата привилегированного потока	1 Наличие ошибок в программном коде криптографических средств
			2 Отсутствие аутентификации при подключении к закрытому каналу
Оборудование ЛВС открытого контура	99 у.е.	Перехват передаваемых сообщений	1 Неправильная конфигурация средств криптографических

			средств защиты информации
			2 Использование алгоритмов шифрования с недостаточной длиной ключа
		Модификация и удаление передаваемых сообщений	1 Отсутствие алгоритмов аутентификации
			2 Использование устаревшего алгоритма аутентификации
		Прослушивание привилегированного трафика	1 Отсутствие криптографической защиты, применяемой к пакетам данных
			2 Отсутствие контроля доступа к защищенному каналу
Оборудование ЛВС закрытого контура	85 у.е.	Прослушивание привилегированного трафика	1 Отсутствие криптографической защиты, применяемой к пакетам данных
			2 Отсутствие контроля доступа к защищенному каналу
		Модификация и удаление передаваемых сообщений	1 Отсутствие алгоритмов аутентификации
			2 Использование устаревшего алгоритма аутентификации
			1 Неправильная конфигурация средств

		Перехват передаваемых сообщений	криптографических средств защиты информации
			2 Отсутствие регламента смены пароля

4.2 Информационные ресурсы

Таблица 2 - Модели угроз для информационных ресурсов

Ресурс	Критичность	Угрозы	Уязвимости
БД	50 у.е.	Открытые резервные копии баз данных	1 Отсутствие аудита резервных копий
			2 Отсутствие шифрование резервных копий
		Получение конфиденциальных данных	1 Отсутствие шифрования данных
			2 Отсутствие разграничения прав доступа

4.3 Программные ресурсы

Таблица 3 - Модели угроз для программных ресурсов

Ресурс	Критичность	Угрозы	Уязвимости
ОС	100 у.е.	Угроза несанкционированного доступа	1 Некорректная настройка прав доступа
			2 Перебор паролей
		Сканирование файловой системы	1 Ошибки администрирования системы

СУБД	50 у.е.	Применение SQL-инъекций	1 Отсутствие правил фильтрации SQL-запросов
		Угроза несанкционированного доступа	1 Некорректная настройка прав доступа
			2 Использование устаревших алгоритмов аутентификации для хранения паролей
Прикладное ПО	80 у.е.	Неавторизованный доступ к ПО	1 Отсутствие разграничения прав доступа
		Отказ в обслуживании	1 Ошибки разработчиков

Задание вероятности и критичности для каждой угрозы

4.4 Аппаратные ресурсы

Таблица 4 - Задание вероятности и критичности для аппаратных ресурсов

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
Сервер закрытого контура		
Угроза 1/Уязвимость 1	90	60
Угроза 1/Уязвимость 2	86	50
Угроза 2/Уязвимость 1	80	70
Угроза 2/Уязвимость 2	75	35
Угроза 3/Уязвимость 1	80	40
Угроза 3/Уязвимость 2	80	80
Сервер открытого контура		

Угроза 1/Уязвимость 1	50	50
Угроза 1/Уязвимость 2	75	70
Угроза 1/Уязвимость 3	90	10
Угроза 2/Уязвимость 1	80	20
Угроза 2/Уязвимость 2	85	60
Угроза 3/Уязвимость 1	80	55
МЭ открытого контура		
Угроза 1/Уязвимость 1	90	60
Угроза 1/Уязвимость 2	80	50
Угроза 2/Уязвимость 1	75	30
Угроза 2/Уязвимость 2	85	30
Угроза 3/Уязвимость 1	70	30
Угроза 3/Уязвимость 2	70	45
СКЗИ закрытого контура		
Угроза 1/Уязвимость 1	70	70
Угроза 1/Уязвимость 2	75	20
Угроза 2/Уязвимость 1	85	10
Угроза 2/Уязвимость 2	90	30
Угроза 3/Уязвимость 1	69	30
Угроза 3/Уязвимость 2	60	60
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	75	40
Угроза 1/Уязвимость 2	90	50
Угроза 2/Уязвимость 1	90	40
Угроза 2/Уязвимость 2	70	45
Угроза 3/Уязвимость 1	80	50
Угроза 3/Уязвимость 2	85	55
Оборудование ЛВС открытого контура		
Угроза 1/Уязвимость 1	90	40
Угроза 1/Уязвимость 2	80	40
Угроза 2/Уязвимость 1	70	45
Угроза 2/Уязвимость 2	78	40
Угроза 3/Уязвимость 1	69	35
Угроза 3/Уязвимость 2	80	30
Оборудование ЛВС закрытого контура		

Угроза 1/Уязвимость 1	70	40
Угроза 1/Уязвимость 2	75	50
Угроза 2/Уязвимость 1	90	30
Угроза 2/Уязвимость 2	75	**70**
Угроза 3/Уязвимость 1	80	70
Угроза 3/Уязвимость 2	90	65

4.5 Информационные ресурсы

Таблица 5 - Задание вероятности и критичности для информационных ресурсов

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
БД		
Угроза 1/Уязвимость 1	90	50
Угроза 1/Уязвимость 2	85	50
Угроза 2/Уязвимость 1	80	70
Угроза 2/Уязвимость 2	75	65

4.6 Программные ресурсы

Таблица 6 - Задание вероятности и критичности для программных ресурсов

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
ОС		
Угроза 1/Уязвимость 1	90	40
Угроза 1/Уязвимость 2	87	30
Угроза 2/Уязвимость 1	80	65
Прикладное ПО		
Угроза 1/Уязвимость 1	70	80
Угроза 2/Уязвимость 1	80	65
СУБД		
Угроза 1/Уязвимость 1	90	45
Угроза 2/Уязвимость 1	87	65
Угроза 2/Уязвимость 2	70	65

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

Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации. Вычисляется одно значение (для суммарной угрозы). Получается значение уровня угрозы по уязвимости в интервале от 0 до 1.

а) для режима с одной базовой угрозой $Th = \frac{ER}{100} \times \frac{P(V)}{100}$,

где ER (%) - критичность реализации угрозы,

$P(V)$ (%) – вероятность реализации угрозы через данную уязвимость

Расчет уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh:

а) для режима с одной базовой угрозой $CTh = 1 - \prod_{n=1}^{N}(1 - Th)$

5.1 Аппаратные ресурсы

Таблица 7 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для аппаратных ресурсов

Угроза/Уязвимость	**Уровень угрозы, Th** $\boldsymbol{Th = \frac{ER}{100} \cdot \frac{P(V)}{100}}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $\boldsymbol{CTh = 1 - \prod_{n=1}^{n}(1 - Th)}$
Сервер закрытого контура		
Угроза 1/Уязвимость 1	0,540	0,737
Угроза 1/Уязвимость 2	0,430	
Угроза 2/Уязвимость 1	0,560	0,675
Угроза 2/Уязвимость 2	0,263	
Угроза 3/Уязвимость 1	0,320	0,755
Угроза 3/Уязвимость 2	0,640	
Сервер открытого контура		

Угроза 1/Уязвимость 1	0,250	0,675
Угроза 1/Уязвимость 2	0,525	
Угроза 1/Уязвимость 3	0,090	
Угроза 2/Уязвимость 1	0,160	0,588
Угроза 2/Уязвимость 2	0,510	
Угроза 3/Уязвимость 1	0,440	0,440
МЭ открытого контура		
Угроза 1/Уязвимость 1	0,540	0,724
Угроза 1/Уязвимость 2	0,400	
Угроза 2/Уязвимость 1	0,225	0,422
Угроза 2/Уязвимость 2	0,255	
Угроза 3/Уязвимость 1	0,210	0,458
Угроза 3/Уязвимость 2	0,315	
СКЗИ закрытого контура		
Угроза 1/Уязвимость 1	0,490	0,566
Угроза 1/Уязвимость 2	0,150	
Угроза 2/Уязвимость 1	0,085	0,332
Угроза 2/Уязвимость 2	0,270	
Угроза 3/Уязвимость 1	0,207	0,492
Угроза 3/Уязвимость 2	0,360	
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	0,300	0,615
Угроза 1/Уязвимость 2	0,450	
Угроза 2/Уязвимость 1	0,360	0,561
Угроза 2/Уязвимость 2	0,315	
Угроза 3/Уязвимость 1	0,400	0,680
Угроза 3/Уязвимость 2	0,468	
Оборудование ЛВС открытого контура		
Угроза 1/Уязвимость 1	0,360	0,564
Угроза 1/Уязвимость 2	0,320	
Угроза 2/Уязвимость 1	0,315	0,528
Угроза 2/Уязвимость 2	0,312	
Угроза 3/Уязвимость 1	0,242	0,423
Угроза 3/Уязвимость 2	0,240	
Оборудование ЛВС закрытого контура		

Угроза 1/Уязвимость 1	0,280	0,55
Угроза 1/Уязвимость 2	0,375	
Угроза 2/Уязвимость 1	0,270	0,653
Угроза 2/Уязвимость 2	0,525	
Угроза 3/Уязвимость 1	0,560	0,817
Угроза 3/Уязвимость 2	0,585	

5.2 Информационные ресурсы

Таблица 8 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для информациорнных ресурсов

Угроза/Уязвимость	**Уровень угрозы, Th** $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $CTh = 1 - \prod_{n=1}^{n}(1 - Th)$
БД		
Угроза 1/Уязвимость 1	0,450	0,683
Угроза 1/Уязвимость 2	0,425	
Угроза 2/Уязвимость 1	0,560	0,774
Угроза 2/Уязвимость 2	0,488	

5.3 Программные ресурсы

Таблица 9 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для программных ресурсов

Угроза/Уязвимость	**Уровень угрозы, Th** $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $CTh = 1 - \prod_{n=1}^{n}(1 - Th)$
ОС		
Угроза 1/Уязвимость 1	0,360	0,527
Угроза 1/Уязвимость 2	0,261	
Угроза 2/Уязвимость 1	0,520	0.520
Прикладное ПО		
Угроза 1/Уязвимость 1	0,560	0,560
Угроза 2/Уязвимость 1	0,520	0,520
СУБД		
Угроза 1/Уязвимость 1	0,405	0,405
Угроза 2/Уязвимость 1	0,566	0,763
Угроза 2/Уязвимость 2	0,455	

Расчет общего уровня угроз и риска каждого ресурса

Рассчитать общий уровень угроз по ресурсу $CThR$:

а) для режима с одной базовой угрозой $CThR = 1 - \prod_{n=1}^{N}(1 - Th)$

Рассчитать риск ресурса R:

а) для режима с одной базовой угрозой $R_{old} = CThR * D$

где D – критичность ресурса для одной базовой угрозы. Задается в деньгах или уровнях.

5.4 Аппаратные ресурсы

Таблица 10 - Расчет общего уровня угроз и риска для аппаратных ресурсов

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{old}**

		$R_{old} = CThR \cdot D$
Сервер закрытого контура		
Угроза 1/Уязвимость 1	0,979	97,9
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Сервер открытого контура		
Угроза 1/Уязвимость 1	0,925	111
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
МЭ открытого контура		
Угроза 1/Уязвимость 1	0,913	73,04
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
СКЗИ закрытого контура		
Угроза 1/Уязвимость 1	0,853	42,65
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	0,946	69,058
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Оборудование ЛВС открытого контура		

Угроза 1/Уязвимость 1	0,881	87,219
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Оборудование ЛВС закрытого контура		
Угроза 1/Уязвимость 1	0,971	82,535
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

5.5 Информационные ресурсы

Таблица 11 - Расчет общего уровня угроз и риска для информационных ресурсов

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{old}** $R_{old} = CThR \cdot D$
БД		
Угроза 1/Уязвимость 1	0,928	46,4
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		

5.6 Программные ресурсы

Таблица 12 - Расчет общего уровня угроз и риска для программных ресурсов

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{old}** $R_{old} = CThR \cdot D$
ОС		
Угроза 1/Уязвимость 1	0,772	77,2
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Прикладное ПО		
Угроза 1/Уязвимость 1	0,788	39,4
Угроза 2/Уязвимость 1		
СУБД		
Угроза 1/Уязвимость 1	0,859	68,72
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		

Контрмеры

6.1 Аппаратные ресурсы

● 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.

6.2 Информационные ресурсы

- Ведение аудита резервных копий
- Ведение шифрования резервных копий
- Ведение шифрования данных, хранимых на БД
- Разграничение прав доступа, введение ролевую систему доступа

6.3 Программные ресурсы

- Разграничение прав доступа, введение ролевую систему доступа
- Ввести ограниченное количество попыток входа и минимальный и максимальный срок действия пароля
- Вести аудит системы
- Введение правил фильтрации SQL-запросов
- Настроить более современные алгоритмы шифрования
- Регулярное обновление ПО и ОС

Задание вероятности и критичности для каждой угрозы с учетом контрмер

7.1 Аппаратные ресурсы

Таблица 13 - Задание вероятности и критичности для аппаратных ресурсов с учетом контрмер

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
Сервер закрытого контура		
Угроза 1/Уязвимость 1	1	60
Угроза 1/Уязвимость 2	2	50
Угроза 2/Уязвимость 1	3	70
Угроза 2/Уязвимость 2	3	35
Угроза 3/Уязвимость 1	4	40
Угроза 3/Уязвимость 2	5	80
Сервер открытого контура		

Угроза 1/Уязвимость 1	4	50
Угроза 1/Уязвимость 2	3	70
Угроза 1/Уязвимость 3	6	10
Угроза 2/Уязвимость 1	5	20
Угроза 2/Уязвимость 2	7	60
Угроза 3/Уязвимость 1	4	55
МЭ открытого контура		
Угроза 1/Уязвимость 1	7	60
Угроза 1/Уязвимость 2	2	50
Угроза 2/Уязвимость 1	6	30
Угроза 2/Уязвимость 2	5	30
Угроза 3/Уязвимость 1	5	30
Угроза 3/Уязвимость 2	3	45
СКЗИ закрытого контура		
Угроза 1/Уязвимость 1	6	70
Угроза 1/Уязвимость 2	6	20
Угроза 2/Уязвимость 1	7	10
Угроза 2/Уязвимость 2	8	30
Угроза 3/Уязвимость 1	5	30
Угроза 3/Уязвимость 2	3	60
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	3	40
Угроза 1/Уязвимость 2	3	50
Угроза 2/Уязвимость 1	6	40
Угроза 2/Уязвимость 2	1	45
Угроза 3/Уязвимость 1	4	50
Угроза 3/Уязвимость 2	3	55
Оборудование ЛВС открытого контура		
Угроза 1/Уязвимость 1	5	40
Угроза 1/Уязвимость 2	6	40
Угроза 2/Уязвимость 1	6	45
Угроза 2/Уязвимость 2	7	40
Угроза 3/Уязвимость 1	8	35
Угроза 3/Уязвимость 2	3	30
Оборудование ЛВС закрытого контура		

Угроза 1/Уязвимость 1	3	40
Угроза 1/Уязвимость 2	3	50
Угроза 2/Уязвимость 1	5	30
Угроза 2/Уязвимость 2	6	**70**
Угроза 3/Уязвимость 1	7	70
Угроза 3/Уязвимость 2	5	65

7.2 Информационные ресурсы

Таблица 14 - Задание вероятности и критичности для информационных ресурсов с учетом контрмер

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
БД		
Угроза 1/Уязвимость 1	6	50
Угроза 1/Уязвимость 2	7	50
Угроза 2/Уязвимость 1	2	70
Угроза 2/Уязвимость 2	3	65

7.3 Программные ресурсы

Таблица 15 - Задание вероятности и критичности для программных ресурсов с учетом контрмер

Угроза/Уязвимость	**Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)**	**Критичность реализации угрозы через уязвимость (%), ER**
ОС		
Угроза 1/Уязвимость 1	5	40
Угроза 1/Уязвимость 2	3	30
Угроза 2/Уязвимость 1	7	65
Прикладное ПО		
Угроза 1/Уязвимость 1	2	80
Угроза 2/Уязвимость 1	3	65
СУБД		
Угроза 1/Уязвимость 1	2	45
Угроза 2/Уязвимость 1	5	65
Угроза 2/Уязвимость 2	3	65

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

8.1 Аппаратные ресурсы

Таблица 16 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для аппаратных ресурсов с учетом контрмер

Угроза/Уязвимость	**Уровень угрозы, Th** $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $CTh = 1 - \prod_{n=1}^{n}(1 - Th)$
Сервер закрытого контура		
Угроза 1/Уязвимость 1	0,006	0,015
Угроза 1/Уязвимость 2	0,010	
Угроза 2/Уязвимость 1	0,021	0,031
Угроза 2/Уязвимость 2	0,011	
Угроза 3/Уязвимость 1	0,016	0,055
Угроза 3/Уязвимость 2	0,040	
Сервер открытого контура		
Угроза 1/Уязвимость 1	0,020	0,046
Угроза 1/Уязвимость 2	0,021	
Угроза 1/Уязвимость 3	0,006	
Угроза 2/Уязвимость 1	0,010	0,051
Угроза 2/Уязвимость 2	0,042	
Угроза 3/Уязвимость 1	0,022	0,022
МЭ открытого контура		

Угроза 1/Уязвимость 1	0,042	0,005
Угроза 1/Уязвимость 2	0,010	
Угроза 2/Уязвимость 1	0,018	0,032
Угроза 2/Уязвимость 2	0,015	
Угроза 3/Уязвимость 1	0,015	0,028
Угроза 3/Уязвимость 2	0,014	
СКЗИ закрытого контура		
Угроза 1/Уязвимость 1	0,042	0,053
Угроза 1/Уязвимость 2	0,012	
Угроза 2/Уязвимость 1	0,007	0,030
Угроза 2/Уязвимость 2	0,024	
Угроза 3/Уязвимость 1	0,015	0,032
Угроза 3/Уязвимость 2	0,018	
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	0,012	0,026
Угроза 1/Уязвимость 2	0,015	
Угроза 2/Уязвимость 1	0,024	0,028
Угроза 2/Уязвимость 2	0,005	
Угроза 3/Уязвимость 1	0,020	0,036
Угроза 3/Уязвимость 2	0,017	
Оборудование ЛВС открытого контура		
Угроза 1/Уязвимость 1	0,020	0,043
Угроза 1/Уязвимость 2	0,024	
Угроза 2/Уязвимость 1	0,027	0,054
Угроза 2/Уязвимость 2	0,028	
Угроза 3/Уязвимость 1	0,028	0,036
Угроза 3/Уязвимость 2	0,009	
Оборудование ЛВС закрытого контура		
Угроза 1/Уязвимость 1	0,012	0,026
Угроза 1/Уязвимость 2	0,015	
Угроза 2/Уязвимость 1	0,015	0,056
Угроза 2/Уязвимость 2	0,042	
Угроза 3/Уязвимость 1	0,049	0,079
Угроза 3/Уязвимость 2	0,033	

8.2 Информационные ресурсы

Таблица 17 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для информационных ресурсов с учетом контрмер

Угроза/Уязвимость	**Уровень угрозы, Th** $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $CTh = 1 - \prod_{n=1}^{n}(1 - Th)$
БД		
Угроза 1/Уязвимость 1	0,030	0,063
Угроза 1/Уязвимость 2	0,035	
Угроза 2/Уязвимость 1	0,014	0,033
Угроза 2/Уязвимость 2	0,020	

8.3 Программные ресурсы

Таблица 18 - Расчёт уровня угрозы по уязвимости и уровня угрозы по всем уязвимостям для программных ресурсов с учетом контрмер

Угроза/Уязвимость	**Уровень угрозы, Th** $Th = \frac{ER}{100} \cdot \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза, CTh** $CTh = 1 - \prod_{n=1}^{n}(1 - Th)$
ОС		
Угроза 1/Уязвимость 1	0,020	0,029
Угроза 1/Уязвимость 2	0,009	
Угроза 2/Уязвимость 1	0,046	0,046
Прикладное ПО		
Угроза 1/Уязвимость 1	0,016	0,016
Угроза 2/Уязвимость 1	0,020	0,020
СУБД		
Угроза 1/Уязвимость 1	0,009	0,009
Угроза 2/Уязвимость 1	0,033	0,051
Угроза 2/Уязвимость 2	0,020	

Повторный расчет общего уровня угроз и риска каждого ресурса с учетом контрмер

9.1 Аппаратные ресурсы

Таблица 19 - Расчет общего уровня угроз и риска для аппаратных ресурсов с учетом контрмер

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{new}** $R_{new} = CThR \cdot D$
Сервер закрытого контура		
Угроза 1/Уязвимость 1	0,099	9,9
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Сервер открытого контура		
Угроза 1/Уязвимость 1	0,115	13,8
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
МЭ открытого контура		
Угроза 1/Уязвимость 1	0,108	8,64
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
СКЗИ закрытого контура		

Угроза 1/Уязвимость 1	0,112	5,6
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Однонаправленный МЭ		
Угроза 1/Уязвимость 1	0,088	6,424
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Оборудование ЛВС открытого контура		
Угроза 1/Уязвимость 1	0,128	12,672
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Оборудование ЛВС закрытого контура		
Угроза 1/Уязвимость 1	0,155	13,175
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

9.2 Информационные ресурсы

Таблица 20 - Расчет общего уровня угроз и риска для информационных ресурсов с учетом контрмер

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{new}** $R_{new} = CThR \cdot D$
БД		
Угроза 1/Уязвимость 1	0,095	4,75
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		

9.3 Программные ресурсы

Таблица 21 - Расчет общего уровня угроз и риска для программных ресурсов с учетом контрмер

Угроза/Уязвимость	**Общий уровень угроз по ресурсу (%), $CThR$** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	**Риск ресурса для режима с одной общей угрозой (%), R_{new}** $R_{new} = CThR \cdot D$
ОС		
Угроза 1/Уязвимость 1	0,073	7,3
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Прикладное ПО		
Угроза 1/Уязвимость 1	0,035	1,75
Угроза 2/Уязвимость 1		
СУБД		
Угроза 1/Уязвимость 1	0,05	4
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		

Расчет эффективности введения контрмер

Таблица 22 - Расчет эффективности введения контрмер

Ресурс	**Эффективность $E = \frac{R_{old} - R_{new}}{R_{old}}$**
Аппаратные ресурсы	
Сервер закрытого контура	0,9

Сервер открытого контура	0,89
МЭ открытого контура	0,88
СКЗИ закрытого контура	0,88
Однонаправленный МЭ	0,91
Оборудование ЛВС открытого контура	0,86
Оборудование ЛВС закрытого контура	0,85
Программные ресурсы	
Операционная система	0,91
СУБД	0,96
Прикладное ПО	0,94
Информационные ресурсы	
БД	0,90

Выводы: в ходе выполнения лабораторной работы построена модель угроз и уязвимостей для аппаратных, информационных и программных ресурсов ИС.

Проведена оценка риска по каждому ресурсу. После принятия контрмер уровень риска по каждому из ресурсов заметно снизился. Достигнут уровень эффективности снижения риска до приемлемого уровня в 10%.

Оценка рисков необходимо, чтобы выявить существующие риски и оценить их величину. Принятие контрмер необходимо, т.к они уменьшают уровень риска, а, значит, снижают возможность нарушения целостности, конфиденциальности и доступности информации, а также снизить убытки и простой системы.