



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт комплексной безопасности и специального приборостроения
КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт
по практической работе
по дисциплине «Управление информационной
безопасностью»
на тему: «Расчет рисков ИБ»

Выполнил студент:
Группы: ББМО-02-22
Исаев А.М.

Проверил: Пимонов Р.В.

Москва 2022

В рамках данной практической работы предстоит рассчитать риски ИБ организации(ГК Иннохет), определить объект, угрозу и уязвимости и рассчитать риски ИБ, отобразить расчеты и определить рекомендационные меры.

Перечислим ресурсы, угрозы и уязвимости. Они представлены в таблице 1.

Таблица 1 – Ресурсы, угрозы и уязвимости организации

Объект	Угроза	Уязвимость
ИСПДН «ГК Иннохет»	Несанкционированный доступ к ресурсам	Отсутствие мер разграничения пользователей
		Слабая система аутентификации
	Утечка конфиденциальных данных	Недостатки в системах управления доступом
		Отсутствие шифрования данных
	Угроза целостности данных	Возможность изменения данных
		Отсутствие проверки целостности данных в кеше

2 объект - Информационная система для обработки финансовой информации "Гк Иннохет"

Объект	Угроза	Уязвимость
Информационная система обработки финансовой информации "Гк Иннохет"	DDOS-атаки	Отсутствие мер защиты от DDOS
		Недостаточная пропускная способности сети
	Нарушение доступности данных	Недостатки в системах управления доступом
		Отсутствие шифрования данных
	Угроза потенциального несанкционированного проникновения в ресурсы организации со стороны внешних агентов или хакеров, действующих из другой страны.	Недостатки в настройке виртуальной приватной сети

		Недостатки в мониторинге и обнаружении инцидентов
--	--	---

Третий объект – сервер, на котором хранится БД ИСПДН «Гк Иннохет»

Объект	Угроза	Уязвимость
Сервер хранения БД ИСПДН «Гк Иннохет»	Отказ в обслуживании из-за технических сбоев	Отсутствие мер защиты
		Использование серверов с недостаточной вычислительной мощностью
	Атаки на сотрудников организации	Отсутствие систем анализа поведения пользователей и объектов в сети
		Отсутствие обучения по ИБ
	Отсутствие мер по обеспечению безопасности сервера в целом	Устаревшее ПО

		Неэффективные шифровальные методы
--	--	---

Далее, необходимо сформировать входные данные для расчета рисков ИБ.

Входные данные для расчета рисков для объекта 1		
Угроза/Уязвимость	Вероятность реализации угрозы через уязвимость в течении года % P(V)	Критичность реализации угрозы через уязвимость % ER
Угроза 1/ Уязвимость 1	45	50
Угроза 1/ Уязвимость 2	50	60
Угроза 2/ Уязвимость 1	45	65
Угроза 2/ Уязвимость 2	20	25
Угроза 3/ Уязвимость 1	30	50
Угроза 3/ Уязвимость 2	45	50

Входные данные для расчета рисков для объекта 2		
Угроза/Уязвимость	Вероятность реализации угрозы через уязвимость в течении года % P(V)	Критичность реализации угрозы через уязвимость
Угроза 1/ Уязвимость 1	60	75
Угроза 1/ Уязвимость 2	30	35
Угроза 2/ Уязвимость 1	45	60
Угроза 2/ Уязвимость 2	45	55
Угроза 3/ Уязвимость 1	65	80
Угроза 3/ Уязвимость 2	25	40

Входные данные для расчета рисков для объекта 3		
Угроза/Уязвимость	Вероятность реализации угрозы через уязвимость в течении года % P(V)	Критичность реализации угрозы через уязвимость

Угроза 1/ Уязвимость 1	35	60
Угроза 1/ Уязвимость 2	70	80
Угроза 2/ Уязвимость 1	40	60
Угроза 2/ Уязвимость 2	50	55
Угроза 3/ Уязвимость 1	70	80
Угроза 3/ Уязвимость 2	70	80

Далее, необходимо рассчитать общий уровень угроз, действующего на объект Th и уровень угрозы по всем уязвимостям для каждого объекта

Объект 1

Угроза/Уязвимость	Уровень угроз % Tr $TR = \frac{ER}{100} * \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям $C_{Th}=1- \Pi(1-Th)$
Угроза 1/ Уязвимость 1	0,22	0,45
Угроза 1/ Уязвимость 2	0,3	

Угроза 2/ Уязвимость 1	0,29	0.3255
Угроза 2/ Уязвимость 2	0,05	
Угроза 3/ Уязвимость 1	0,15	0,33
Угроза 3/ Уязвимость 2	0,22	

Объект 2

Угроза/Уязвимость	Уровень угроз % Tr $TR = ER/100 * P(V)/100$	Уровень угрозы по всем уязвимостям $C_{Th}=1- \Pi(1-Th)$
Угроза 1/ Уязвимость 1	0,44	0.49
Угроза 1/ Уязвимость 2	0,10	
Угроза 2/ Уязвимость 1	0,27	0.44
Угроза 2/ Уязвимость 2	0,24	
Угроза 3/ Уязвимость 1	0,52	0.56

Угроза 3/ Уязвимость 2	0,1	
---------------------------	-----	--

Объект 3

Угроза/Уязвимость	Уровень угроз % Tr $TR = ER/100 * P(V)/100$	Уровень угрозы по всем уязвимостям $C_{Th}=1- \Pi(1-Th)$
Угроза 1/ Уязвимость 1	0,21	0.644
Угроза 1/ Уязвимость 2	0,55	
Угроза 2/ Уязвимость 1	0,24	0.445
Угроза 2/ Уязвимость 2	0,27	
Угроза 3/ Уязвимость 1	0,55	0.797
Угроза 3/ Уязвимость 2	0,55	

Далее, для каждого объекта необходимо рассчитать $C_{Th}R$ – Общий уровень угроз и риск по объекту – R

Объект 1

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям CTh=1- П(1-Th)	Общий уровень угроз CThR %	Риск по ресурсу R
Угроза 1/ Уязвимость 1	0,45	0,7514	75,14
Угроза 1/ Уязвимость 2			
Угроза 2/ Уязвимость 1	0.3255		
Угроза 2/ Уязвимость 2			
Угроза 3/ Уязвимость 1	0,33		
Угроза 3/ Уязвимость 2			

Объект 2

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям $C_{Th}=1 - \Pi(1 - T_h)$	Общий уровень угроз $C_{Th}R$ %	Риск по ресурсу R
Угроза 1/ Уязвимость 1	0.49	0,87336	87.73

Угроза 1/ Уязвимость 2			
Угроза 2/ Уязвимость 1	0.44		
Угроза 2/ Уязвимость 2			
Угроза 3/ Уязвимость 1	0.56		
Угроза 3/ Уязвимость 2			

Объект 3

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям $C_{Th}=1 - \Pi(1-Th)$	Общий уровень угроз $C_{Th}R$ %	Риск по ресурсу R
Угроза 1/ Уязвимость 1	0.644	0,9598	95.98
Угроза 1/ Уязвимость 2			
Угроза 2/ Уязвимость 1	0.445		

Угроза 2/ Уязвимость 2			
Угроза 3/ Уязвимость 1	0.797		
Угроза 3/ Уязвимость 2			

В результате вычислений – риск по ресурсам равен 258,85 у.е

Рекомендации по улучшению мер защиты объекта

1) Необходимо применение фильтрацию трафика и CDN для защиты от DDoS, а также использование резервных систем для поддержания доступности данных.

2) Необходимо шифрование конфиденциальных данные и применение механизмов двухфакторной аутентификации для предотвращения несанкционированного доступа

3) Необходимо создавать резервные копии данных.

4) Необходимо внедрять системы мониторинга на случай нештатных ситуаций.

5) Необходимо проведение обучения по безопасности информации для сотрудников и внедрение строгих политик контроля доступа.

В ходе работы был проведен расчет рисков ИСПДн «Гк Иннохет», данные рекомендации по улучшению мер защиты объекта а общий риск равен 258,85 условных единицам.