МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Практическая работа № 1.10

по дисциплине

«Управление информационной безопасностью»

Выполнил:

ББМО–01–22

Чадов В. Т.

Проверил:

Пимонов Р. В.

«Зачтено» «__»_____2023 г. _____

Москва 2023

Содержание

РАСЧЁТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Входные данные

В данной практической работе производится расчёт рисков информационной безопасности для организации ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”. Исходные данные возьмем из практический работ 1.3 “Создание политики информационной безопасности”, 1.6 “Построение модели нарушителя” и 1.8. “Построение модели угроз”. Будем анализировать ресурс “Информационные системы Организации”. Входные данные по ресурсам, угрозам и уязвимостям ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ” представлены в таблице 1.

Таблица 1 – Входные данные по ресурсам, угрозам и уязвимостям ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”

Ресурс	Угрозы	Уязвимости
Информационные системы Организации	Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну	Уволенные сотрудники
		Нечёткие формулировки в регламенте о разглашении информации
		Недостаточное шифрование данных при передаче по сети
	Саботаж текущих проектов	Отсутствие средств защиты от DDoS-атак, недостаточная пропускная способность интернет-канала
		Вывод из строя оборудования посредством взлома (вируса)

		Старое ПО, отсутствие обновления средств информационной безопасности
		Кража, реверс инжиниринг материальных носителей информации с целью получения данных
	Срыв запланированной сделки с партнером	Модификация информации и отправка её с недостоверной информацией от имени Организации и её сотрудников
	Изменение продукта, предназначенного для государственной структуры с целью шпионажа или саботажа	Взлом информационных систем с целью модификации продуктов, производимых организацией
	Разглашение персональных данных граждан	Утечка идентификационной информации граждан из базы данных

Отобразим вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость для каждого ресурса ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ” в таблице 2.

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”

Работники организации		
Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER
Угроза 1 /Уязвимость 1	70	40
Угроза 1 /Уязвимость 2	20	20
Угроза 1 /Уязвимость 3	10	80
Угроза 2 /Уязвимость 1	20	70
Угроза 2 /Уязвимость 2	20	70
Угроза 2 /Уязвимость 3	10	40
Угроза 2 /Уязвимость 4	20	40
Угроза 3 /Уязвимость 1	10	50
Угроза 4 /Уязвимость 1	10	90
Угроза 5 /Уязвимость 1	10	20

Расчет рисков

Отобразим результаты расчёта уровня угрозы по каждой уязвимости, уровня угрозы по всем уязвимостям, через которые она может быть реализована, общего уровня угроз по ресурсу и риска по ресурсу для каждого ресурса ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ” в таблице 3. Критичность ресурса (D) для “Информационные системы Организации” равна 100%. Уровень принятия риска менее 50%.

Таблица 3 – Расчет рисков информационной безопасности для ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”

Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	Общий уровень угроз по ресурсу %, CThR	Риск по ресурсу, у.е
Угроза 1 /Уязвимость 1	70%	40%	28%	36,41%	64,81%	64,81%
Угроза 1 /Уязвимость 2	20%	20%	4%			
Угроза 1 /Уязвимость 3	10%	80%	8%			
Угроза 2 /Уязвимость 1	20%	70%	14%	34,68%		
Угроза 2 /Уязвимость 2	20%	70%	14%			
Угроза 2 /Уязвимость 3	10%	40%	4%			
Угроза 2 /Уязвимость 4	20%	40%	8%			
Угроза 3 /Уязвимость 1	10%	50%	5%	5%		
Угроза 4 /Уязвимость 1	10%	90%	9%	9%		
Угроза 5 /Уязвимость 1	10%	20%	2%	2%		

Рекомендации по улучшению мер защиты

1. Внести правки в регламент о разглашении информации, чтобы изложенная там информация была понятна читателю.
2. Организовать шифрование данных, распространить приватные ключи.
3. Внедрение актуальных технических решений для контроля и мониторинга информационных ресурсов организации.
4. Регулярно обновлять программное обеспечение и устанавливать патчи безопасности.
5. Применение при разработке методик затрудняющий реверс-инжиниринг разработанных устройств и ПО.
6. Разделение информации между сотрудниками, улучшение правил систем разграничения доступа.
7. Реализовать механизмы защиты от Dos/DDoS атак.
8. Установка антивирусного ПО на все используемое оборудование.

Повторный расчет рисков

После применения рекомендаций перерасчитаем риски. Отобразим результаты расчёта уровня угрозы по каждой уязвимости, уровня угрозы по всем уязвимостям, через которые она может быть реализована, общего уровня угроз по ресурсу и риска по ресурсу для каждого ресурса ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ” в таблице 4. Критичность ресурса (D) для “Информационные системы Организации” равна 100%.

Таблица 4 – Повторный расчет рисков информационной безопасности для ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”

Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	Общий уровень угроз по ресурсу %, CThR	Риск по ресурсу, у.е
Угроза 1 /Уязвимость 1	40%	40%	16,00%	20,17%	45,02%	45,02%
Угроза 1 /Уязвимость 2	5%	20%	1,00%			
Угроза 1 /Уязвимость 3	5%	80%	4,00%			
Угроза 2 /Уязвимость 1	15%	70%	10,50%	23,32%		
Угроза 2 /Уязвимость 2	10%	70%	7,00%			
Угроза 2 /Уязвимость 3	5%	40%	2,00%			
Угроза 2 /Уязвимость 4	15%	40%	6,00%			
Угроза 3 /Уязвимость 1	10%	50%	5,00%	5,00%		
Угроза 4 /Уязвимость 1	5%	90%	4,50%	4,50%		
Угроза 5 /Уязвимость 1	5%	20%	1,00%	1,00%		

После применения рекомендаций риск снизился с 64,81% до 45,02% и теперь соответствует уровню принятия риска менее 50%.