МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа № 4

«Расчёт рисков по информационной системе»

по дисциплине

«Управление информационной безопасностью»

Группа:
ББМО-01-22
Выполнила:
Огольцова Н.Д.

Проверил:
Пимонов Р.В.

Москва

2023

Ресурс: ЦОД		
№	Угроза	Уязвимость
1	Утечка конфиденциальной информации или отдельных файлов (нарушение конфиденциальности)	Некомпетентность сотрудников в работе с защищаемой информацией
		Уволенные сотрудники
2	Несанкционированный доступ к компонентам защищаемой информации, системным, конфигурационным, иным служебным данным	Отсутствие строгой настройки привилегий
		Возможность получения доступа из внешний ресурсов
3	Отказ в обслуживании компонентов (нарушение доступности)	Низкий уровень технической защиты и кибербезопасности
Ресурс: Сервер		
№	Угроза	Уязвимость
1	Отказ в обслуживании компонентов (нарушение доступности)	Отсутствие РК (резервного копирования) сервера
2	Несанкционированный доступ к компонентам защищаемой информации, системным, конфигурационным, иным служебным данным	Отсутствие механизмов защиты от DoS/DDoS
Ресурс: Информационная система персональных данных		
1	Несанкционированный доступ к ресурсам сервера	Отсутствие двухфакторной аутентификация
		Уволенные сотрудники

		Некомпетентность сотрудников в работе с защищаемой информацией
2	Утечка конфиденциальной информации (нарушение конфиденциальности)	Отсутствие строгой настройки привилегий

Введение основных параметров: вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость.

Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течение года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER
Ресурс: ЦОД		
Угроза 1 / Уязвимость 1	40	60
Угроза 1 / Уязвимость 2	20	60
Угроза 2 / Уязвимость 1	60	30
Угроза 2 / Уязвимость 2	40	50
Угроза 3 / Уязвимость 1	40	30
Ресурс: Сервер		
Угроза 1 / Уязвимость 1	30	60
Угроза 2 / Уязвимость 1	40	70
Ресурс: Информационная система персональных данных		
Угроза 1 / Уязвимость 1	60	60
Угроза 1 / Уязвимость 2	30	70
Угроза 1 / Уязвимость 3	60	50
Угроза 2 / Уязвимость 1	40	50

Расчёт уровня угрозы по каждой уязвимости, уровня угрозы по всем уязвимостям, через которые она может быть реализована и общего уровня угроз по ресурсу.

Угроза/уязвимость	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована, CTh	Общий уровень угроз по ресурсу, CThR
Ресурс: ЦОД			
Угроза 1 / Уязвимость 1	0.24	0.64	0.5
Угроза 1 / Уязвимость 2	0.12		
Угроза 2 / Уязвимость 1	0.18	0.74	
Угроза 2 / Уязвимость 2	0.08		
Угроза 3 / Уязвимость 1	0.12	0.12	
Ресурс: Сервер			
Угроза 1 / Уязвимость 1	0.18	0.18	0.54
Угроза 2 / Уязвимость 1	0.28	0.28	
Ресурс: Информационная система персональных данных			
Угроза 1 / Уязвимость 1	0.36	0.27	0.53
Угроза 1 / Уязвимость 2	0.21		
Угроза 1 / Уязвимость 3	0.3		
Угроза 2 / Уязвимость 1	0.2	0.2	

Расчёт риска по ресурсу и риска по информационной системе.

Угроза/уязвимость	Общий уровень угроз по ресурсу, CThR	Критичность ресурса, D	Оценка уровня %	Риск по ресурсу, R	Риск по ресурсам, CR
Ресурс: ЦОД					
Угроза 1 / Уязвимость 1	0.5	3	100	50	50
Угроза 1 / Уязвимость 2					
Угроза 2 / Уязвимость 1					
Угроза 2 / Уязвимость 2					
Угроза 3 / Уязвимость 1					
Ресурс: Сервер					
Угроза 1 / Уязвимость 1	0.54	3	100	54	54
Угроза 2 / Уязвимость 1					
Ресурс: Информационная система персональных данных					
Угроза 1 / Уязвимость 1	0.53	3	100	53	53
Угроза 1 / Уязвимость 2					
Угроза 1 / Уязвимость 3					
Угроза 2 / Уязвимость 1					

Суммарный риск по информационной системе (CR) получился средним – 43.

К информационной системе необходимо принять меры по улучшению политики безопасности.

Рекомендации:

1. Улучшить программные/программно-аппаратные способы реализации разграничения доступа;
2. Вести обучение по информационной безопасности;
3. Реализовать строгое и своевременное ограничение доступа для увольняющихся сотрудников.