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

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по практической работе №4

по дисциплине: «Управление информационной безопасностью»

на тему: «Расчет рисков информационной безопасности»

Выполнил:

Студент группы ББМО-02-22

Кузьмин Владимир Дмитриевич

Проверил:

Пимонов Роман Владимирович

Москва 2023

СОДЕРЖАНИЕ

ЗАДАНИЕ

Цель работы: Изучить алгоритм оценки рисков «угрозы-уязвимости».

Задачи:

1. Установить ПП «Гриф» для расчета рисков ИБ.
2. Самостоятельно сформировать вероятности реализации на определенных активах Организации угрозы ИБ через уязвимости.
3. Установить уровень принятия риска (например, менее 30%).
4. Провести анализ рисков, выявить ресурс с наиболее высоким уровнем риска, определить уязвимость на ресурсе с наиболее высоким уровнем угрозы.
5. Применить контрмеры для коррекции рисков.
6. Рассчитать итоговый уровень риска ИБ.
7. Определить эффективность применения контрмер.
8. Подготовить отчет.

1. ВХОДНЫЕ ДАННЫЕ (РЕСУРСЫ) ДЛЯ РАСЧЕТА РИСКОВ ИБ

Приступим к расчету рисков информационной безопасности для ИСПДн «Роснефть».

Исходные данные (ресурсы) для расчета рисков ИБ получены из предыдущих работ и приведены в таблице 1.

Таблица 1 – Входные данные (ресурсы) для расчета рисков ИБ

Объект	Угрозы	Уязвимости
1. Информационная система персональных данных «ПАО Роснефть»	1.1. Раскрытие конфиденциальных данных	1.1.1. Слабое шифрование данных
		1.1.2. Недостаточный контроль доступа к данным
	1.2. Несанкционированное проникновение и получение доступа к ресурсам информационной системы	1.2.1. Слабые места в системе аутентификации
		1.2.2. Отсутствие обновлений и патчей безопасности
	1.3. Угрозы, связанные с облачными сервисами	1.3.1. Недостатки в облачной безопасности провайдера
		1.3.2. Недостаточные средства мониторинга и анализа активности в облачной среде
2. ЛВС, в рамках которой работники обеспечивают обмен информацией	2.1. Несанкционированные сетевые доступы и внутренние атаки	2.1.1. Неэффективное управление доступом, недостаточная сегментация сети.
		2.1.2. Отсутствие мониторинга сетевой активности
	2.2. Направленные атаки на уязвимости в приложениях, используемых для обмена информацией	2.2.1. Недостаточная валидация ввода команд
		2.2.2. Недостаточная безопасность кода приложений
	2.3. Недостаточная защита от вирусов, троянов и других форм ВПО внутри сети	2.3.1. Несвоевременные обновления сигнатур вредоносных программ
		2.3.2. Недостаточные меры по фильтрации входящего трафика

3. Сервер, на котором хранятся БД ИСПДн, «ПАО Роснефть»	3.1. Атаки, направленные на обман персонала	3.1.1. Отсутствие обучения и обзоров по безопасности
		3.1.2. Нет механизма для быстрого сообщения о подозрительной активности
	3.2. Массированные атаки с целью перегрузки серверных ресурсов	3.2.1. Использование серверов и сетевого оборудования с недостаточной вычислительной мощностью
		3.2.2. Отсутствие систем мониторинга, способных выявлять аномальный трафик
	3.3. Отсутствие актуальных мер по обеспечению безопасности данных	3.3.1. Неиспользование современных методов шифрования данных на сервере
		3.3.2. Отсутствие актуальных механизмов управления доступом и контроля привилегий

2. РАСЧЕТ РИСКОВ ИБ НА ОСНОВЕ МОДЕЛИ НАРУШИТЕЛЯ И МОДЕЛИ УГРОЗ

Укажем вероятности и критичности реализации угроз через уязвимости в разрезе года для каждого объекта ИСПДн «Роснефть».

Исходные данные для расчета рисков ИБ для объектов ИСПДн «Роснефть» представлены в таблице 2.

Таблица 2 – Исходные вероятности объекта 1

Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течении года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
1. Информационная система персональных данных «ПАО Роснефть»		
1.1/1.1.1	50	70
1.1/1.1.2	25	30
1.2/1.2.1	65	80
1.2/1.2.2	35	50
1.3/1.3.1	60	70
1.3/1.3.2	15	40
2. ЛВС, в рамках которой работники обеспечивают обмен информацией		
2.1/2.1.1	35	50
2.1/2.1.2	80	85
2.2/2.2.1	45	60
2.2/2.2.2	15	50
2.3/2.3.1	30	35
2.3/2.3.2	25	30
3. Сервер, на котором хранятся БД ИСПДн, «ПАО Роснефть»		
3.1/3.1.1	40	75
3.1/3.1.2	50	65
3.2/3.2.1	45	70
3.2/3.2.2	45	55
3.3/3.3.1	40	45
3.3/3.3.2	45	50

После определения исходных данных произведем расчет уровней угроз через уязвимости (Th) и по всем уязвимостям (CTh) для каждого ресурса ИС. Также произведем расчет общего уровня угроз (CThR), действующего на объект и расчет итогового риска по ресурсу (R) для каждого объекта ИСПДн «Роснефть».

Формулы для расчета показателей представлены в таблице 3.

Таблица 3 – Формулы расчета

Показатель	Формула
Уровень угрозы по каждой уязвимости %, Th	$Th = \frac{ER}{100} \times \frac{P(V)}{100}$
Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	$CTh = 1 - \prod_{i=1}^{n}(1 - Th_i)$
Общий уровень угроз по ресурсу %, CThR	$CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i)$
Риск по ресурсу у.е., R	$R = CThR \times D$

Расчетные значения для каждого объекта ИСПДн «Роснефть» представлены в таблице 4.

Таблица 4 – Расчетные значения

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	Риск по ресурсу у.е., R
1. Информационная система персональных данных «ПАО Роснефть»				
1.1/1.1.1	0,35	0,402	0,8716	87,16
1.1/1.1.2	0,08			
1.2/1.2.1	0,52	0,606		
1.2/1.2.2	0,18			
1.3/1.3.1	0,42	0,455		
1.3/1.3.2	0,06			
2. ЛВС, в рамках которой работники обеспечивают обмен информацией				
2.1/2.1.1	0,18	0,738	0,8558	85,58
2.1/2.1.2	0,68			
2.2/2.2.1	0,27	0,328		
2.2/2.2.2	0,08			
2.3/2.3.1	0,11	0,181		
2.3/2.3.2	0,08			
3. Сервер, на котором хранятся БД ИСПДн, «ПАО Роснефть»				
3.1/3.1.1	0,3	0,531	0,8491	84,91
3.1/3.1.2	0,33			
3.2/3.2.1	0,32	0,490		
3.2/3.2.2	0,25			
3.3/3.3.1	0,18	0,369		
3.3/3.3.2	0,23			

Таким образом, в результате расчётов риск по ресурсам (CR) равен 257,65 условных единиц.

3. РЕКОМЕНДАЦИИ ПО УЛУЧШЕНИЮ МЕР ЗАЩИТЫ ОБЪЕКТА ИСПДН

1. Улучшение систем контроля доступа, включая установку видеонаблюдения и биометрических систем аутентификации.

2. Внедрение современных средств защиты информации, таких как межсетевые экраны, антивирусное программное обеспечение и системы обнаружения вторжений.

3. Проведение регулярных обучающих семинаров для сотрудников с целью повышения их осведомленности о правилах работы с конфиденциальной информацией и мерах по ее защите.

4. Разработка и внедрение четких политик и процедур, которые будут регулировать работу с персональными данными и обеспечивать их защиту.

5. Проведение регулярного мониторинга и аудита информационной системы на предмет уязвимостей и возможных угроз.

6. Внедрение систем обнаружения и предотвращения утечек данных (DLP), которые помогут предотвратить несанкционированный доступ к конфиденциальной информации.

7. Внедрение системы управления мобильными устройствами (MDM) для контроля над доступом к корпоративным ресурсам с мобильных устройств.

8. Использование надежных облачных провайдеров и обеспечение строгой аутентификации и авторизации пользователей при доступе к данным в облаке.

9. Создание системы резервного копирования данных и регулярного тестирования процедур восстановления информации в случае возникновения инцидентов.

10. Регулярное обновление и совершенствование мер защиты с учетом новых угроз и технологий, а также проведение регулярных оценок эффективности существующих мер защиты.

ЗАКЛЮЧЕНИЕ

В ходе выполнения практической работы был проведен расчет рисков ИСПДн «Роснефть». Были рассчитаны показатели, необходимые для определения дискретного значения риска. По итогам расчетов риск оказался равен 257,65 условным единицам.