УТВЕРЖДАЮ

Руководитель

И. О. Фамилия

«___» _____ 2024 г.

Расчет рисков информационной безопасности
ООО «Техно-Телеком»

Москва 2024

Расчет рисков информационной безопасности ООО «Техно-Телеком»

В рамках данной практической работы выполняется оценка рисков информационной безопасности для компании ООО «Техно-Телеком». Исходные данные были взяты из ранее проведённых практических исследований. Основное внимание уделяется анализу ресурса «Корпоративная сеть и серверы компании». Все входные данные по ресурсам, угрозам и уязвимостям ООО «Техно-Телеком» представлены в таблице 1.

Таблица 1 – Входные данные по ресурсам, угрозам и уязвимостям ООО «Техно-Телеком»

Ресурс	**Угрозы**	**Уязвимости**
Система управления взаимоотношениями с клиентами (CRM)	Угроза утечки данных	Недостаточная шифровка данных.
		Уязвимости в программном обеспечении CRM
	Угроза Фишинга	Недостаточная осведомленность сотрудников
		Отсутствие многофакторной аутентификации
	Угроза SQL-инъекции	Недостаточная валидация входных данных
		Устарелое программное обеспечение

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для ООО «Техно-Телеком»

Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течение года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
Угроза 1 / Уязвимость 1	40	75
Угроза 1 / Уязвимость 2	30	80
Угроза 2 / Уязвимость 1	60	65
Угроза 2 / Уязвимость 2	35	70
Угроза 3 / Уязвимость 1	50	70
Угроза 3 / Уязвимость 2	25	85

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 в таблице 3.

Таблица 3 – Результаты расчёта уровня угрозы по каждой уязвимости

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 %, CTh	Общий уровень угроз по ресурсу %, CThR
Угроза 1 / Уязвимость 1	40	75	30	46,8	87,4
Угроза 1 / Уязвимость 2	30	80	24		
Угроза 2 / Уязвимость 1	60	65	39	53.9	
Угроза 2 / Уязвимость 2	35	70	24,5		
Угроза 3 / Уязвимость 1	50	70	35	48,8	
Угроза 3 / Уязвимость 2	25	85	21,25		

Рекомендации по улучшению мер защиты

- Внедрение надежной шифровки данных
- Регулярное обновление программного обеспечения
- Обучение сотрудников основам кибербезопасности
- Внедрение многофакторной аутентификации
- Валидация и санитизация входных данных
- Мониторинг и анализ сетевого трафика

Повторный расчет рисков

После применения дополнительных рекомендаций, уровни рисков по каждому из ресурсов компании пересчитаны. Ниже представлены обновленные данные расчёта уровня угроз по каждой уязвимости, включая новые меры защиты.

Таблица 4 – Обновленные данные расчёта уровня угроз по каждой уязвимости

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 %, CTh**	**Общий уровень угроз по ресурсу %, CThR**
Угроза 1 / Уязвимость 1	20	55	11	16,34	47,8
Угроза 1 / Уязвимость 2	10	60	0,6		
Угроза 2 / Уязвимость 1	40	45	18	24,15	
Угроза 2 / Уязвимость 2	15	50	7,5		
Угроза 3 / Уязвимость 1	30	50	15	17,8	
Угроза 3 / Уязвимость 2	5	65	3,25		

В ходе выполнения расчета рисков информационной безопасности для компании ООО «Техно-Телеком» были выявлены ключевые уязвимости и угрозы, присущие корпоративной сети и серверам компании.

Проведенный анализ показал необходимость усиления мер безопасности, в частности:

1. **Шифрование данных**: внедрение надежных алгоритмов шифрования для защиты всех данных, хранящихся и передаваемых в системе. Это предотвращает утечку данных в случае их перехвата.
2. **Использование технических средств информационной безопасности**:
    - Установка систем анализа сетевого трафика для выявления подозрительной активности и потенциальных угроз.
    - Регулярное обновление программного обеспечения для устранения известных уязвимостей.

После внедрения предложенных рекомендаций уровень риска был пересчитан и снизился до допустимого уровня, что свидетельствует об эффективности предложенных мер безопасности. Однако для поддержания этого уровня и адаптации к возможным новым угрозам важно продолжать регулярные проверки и обновления мер защиты, включая:

1. Регулярные аудиты безопасности;
2. Обучение сотрудников;
3. Многофакторная аутентификация;
4. Валидация входных данных;
5. Мониторинг и анализ.

Эти меры помогут поддерживать уровень информационной безопасности на должном уровне и своевременно адаптироваться к новым угрозам, обеспечивая надежную защиту корпоративной сети и серверов ООО «Техно-Телеком».