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 на тему: Расчет рисков информационной безопасности

по дисциплине: «Управление информационной безопасностью»

Выполнил:
Студент группы ББМО-01-22
ФИО: Загороднов Е.А.

Проверил:

Р.В. Пимонов

Москва 2023

Содержание

1. Алгоритм оценки рисков «угрозы-уязвимости»

Оценка рисков по методу «угрозы-уязвимости» является важным компонентом информационной безопасности и позволяет оценить вероятность и потенциальные последствия возможных инцидентов. Ключевые шаги данного алгоритма:

1) Идентификация угроз.

На данном этапе происходит определение всех возможных угроз, которые могут повлиять на вашу информационную систему, включая внутренние и внешние угрозы.

2) Определение уязвимостей.

На данном этапе происходит идентификация уязвимостей в вашей системе, то есть слабые места, которые могут быть использованы злоумышленниками.

3) Оценка вероятности угрозы.

На данном этапе происходит оценка вероятности возникновения каждой угрозы, учитывая исторические данные, текущие тренды и экспертное мнение.

4) Оценка потенциальных последствий.

На данном этапе происходит анализ, а именно какие последствия могут возникнуть в случае успешной реализации угрозы. Это может включать финансовые убытки, утечку данных, ущерб репутации и другие аспекты.

5) Оценка уровня риска.

На данном этапе происходит расчет уровень риска как произведение вероятности угрозы на её потенциальные последствия.

6) Приоритизация рисков.

Здесь происходит упорядочивание рисков в порядке убывания по уровню важности, чтобы определить, на какие из них следует обратить особое внимание.

7) Разработка стратегий управления рисками.

На данном этапе решается, каким образом вы будете управлять высокими рисками. Это может включать в себя принятие риска, устранение уязвимостей или внедрение дополнительных защитных мер.

8) Мониторинг и обновление.

На данном этапе происходит регулярный пересмотр оценки рисков, так как ситуация может измениться со временем, и новые угрозы и уязвимости могут появиться.

9) Разработка планов мероприятий.

Здесь ведется разработка детального плана действий для управления рисками и снижения уязвимостей.

10) Обучение и осведомленность.

На данном этапе происходит обучение персонала и создание культуру информационной безопасности, чтобы уменьшить человеческий фактор как уязвимость в системе.

2. Входные данные(ресурсы) для расчета рисков ИБ

Приступим к расчету рисков информационной безопасности для автоматизированной информационной системы Банка ПАО “ЗенитБанк”

Исходные данные возьмем из практический работ 1.3 “Создание политики информационной безопасности”, 1.6 “Построение модели нарушителя” и 1.8. “Построение модели угроз”.

Обратимся к работам, что взять оттуда исходные данные. Ресурсы взяты из пункта 2.1 практической работы 1.8. “Построение модели угроз” и показаны в таблице 1. Угрозы и возможные уязвимости также взяты из данной практической работы и также отражены в таблице 1.

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

Объект	Угрозы	Уязвимости
Объект 1 ИСПДн ПАО ЗенитБанк	**Угроза 1** НСД к ресурсам ИСПДн	**Уязвимость 1** Оставление устройств разблокированными, недостаточная защита компьютеров и мобильных устройств
		Уязвимость 2 Неправильная настройка и управление правами доступа пользователей и администраторов
	Угроза 2 Утечка конфиденциальной информации, нарушение конфиденциальности клиентов	**Уязвимость 1** Уволенные сотрудники
		Уязвимость 2 Недостаточное шифрование данных
	Угроза 3 Отсутствие строгих политик и процедур удаленной работы	**Уязвимость 1** Использование незащищенных или устаревших протоколов связи при удаленном доступе
		Уязвимость 2 Подключение к общедоступным Wi-Fi сетям без использования защищенных виртуальных частных сетей (VPN)
	Угроза 4 Сбой в сетевой инфраструктуре	**Уязвимость 1** Неэффективные меры предотвращения и защиты от распределенных атак на отказ в обслуживании (DDoS)
		Уязвимость 2 Отсутствие регулярных обновлений и патчей для сетевых устройств
	Угроза 5 Отсутствие строгих процессов управления учетными записями	**Уязвимость 1** Неэффективное журналирование и мониторинг действий пользователей
		Уязвимость 2 Неиспользование автоматизированных средств для эффективного управления жизненным циклом учетных записей

Объект 2 ЛВС, в рамках которой работники обеспечивают обмен информацией	**Угроза 1** НСД и атаки внутри сети	**Уязвимость 1** Неэффективное управление доступом, недостаточная сегментация сети.
		Уязвимость 2 Отсутствие мониторинга действий пользователей
	Угроза 2 Заражение систем вирусами, троянами, шпионскими программами	**Уязвимость 1** Отсутствие или неактуальность антивирусных и антималварных программ,
		Уязвимость 2 необновленное программное обеспечение
	Угроза 3 Атаки на перехват и анализ сетевого трафика	**Уязвимость 1** Неактивированный или слабо защищенный Wi-Fi
		Уязвимость 2 Использование устаревших версий протоколов связи
	Угроза 4 Отсутствие четких и строгих политик безопасности	**Уязвимость 1** Отсутствие четких политик по управлению устройствами
		Уязвимость 2 Отсутствие политики использования безопасных паролей
	Угроза 5 Несанкционированный доступ к физической инфраструктуре	**Уязвимость 1** Отсутствие электронных замков и электронных ключей
		Уязвимость 2 Отсутствие регулярного обновления списков доступа
Объект 3 Сервер, на котором хранятся БД ИСПДн, «ПАО Банк ЗенитБанк»	**Угроза 1** Внешние атаки хакеров	**Уязвимость 1** Недостаточная защита сервера, слабые пароли
		Уязвимость 2 Отсутствие средств защиты от DDoS-атак, недостаточная пропускная способность интернет-канала
	Угроза 2 НСД к серверу, на котором хранятся БД ИСПДн	**Уязвимость 1** Недостаточная защита сетевого трафика
		Уязвимость 2 Отсутствие двухфакторной аутентификации
	Угроза 3 Старое программное обеспечение	**Уязвимость 1** Неблагоприятные настройки безопасности
		Уязвимость 2 Отсутствие регулярных антивирусных обновлений

	Угроза 4 Технические сбои, такие как отказ жестких дисков, проблемы с памятью или другие аппаратные проблемы	**Уязвимость 1** Недостаточная система мониторинга и предупреждения об аномалиях в работе жестких дисков, памяти
		Уязвимость 2 Не проведение регулярных тестов на отказы аппаратуры
	Угроза 5 Возможность несанкционированных изменений в настройках сервера или базы данных	**Уязвимость 1** Отсутствие контроля за сетевыми соединениями и недостаточные средства шифрования
		Уязвимость 2 Использование устаревших методов аутентификации или слабых механизмов защиты

3. Расчет рисков ИБ на основе модели нарушетиля и модели угроз

Отобразим вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость для каждого объекта ИСПДН ПАО “ЗенитБанк”. Входные данные для расчёта рисков информационной безопасности для объекта 1 представлены в таблице 2.

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для объекта 1 ИСПДн ПАО “ЗенитБанк”

Объект 1: ИСПДн ПАО ЗенитБанк»		
Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течении года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
Угроза 1 /Уязвимость 1	30	40
Угроза 1 /Уязвимость 2	70	75
Угроза 2 /Уязвимость 1	25	35
Угроза 2 /Уязвимость 2	30	55
Угроза 3 /Уязвимость 1	50	65
Угроза 3 /Уязвимость 2	30	55
Угроза 4 /Уязвимость 1	25	50
Угроза 4 /Уязвимость 2	30	55
Угроза 5 /Уязвимость 1	15	20
Угроза 5 /Уязвимость 2	30	40

Входные данные для расчёта рисков информационной безопасности для объекта 2 представлены в таблице 3.

Таблица 3 – Входные данные для расчёта рисков информационной безопасности для объекта 2 ЛВС, в рамках которой работники обеспечивают обмен информацией

Объект 2: ЛВС, в рамках которой работники обеспечивают обмен информацией		
Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течении года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
Угроза 1 /Уязвимость 1	45	70
Угроза 1 /Уязвимость 2	70	85
Угроза 2 /Уязвимость 1	15	30
Угроза 2 /Уязвимость 2	25	30
Угроза 3 /Уязвимость 1	15	20
Угроза 3 /Уязвимость 2	25	30
Угроза 4 /Уязвимость 1	30	50
Угроза 4 /Уязвимость 2	40	65
Угроза 5 /Уязвимость 1	30	40
Угроза 5 /Уязвимость 2	25	30

Входные данные для расчёта рисков информационной безопасности для объекта 3 представлены в таблице 4.

Таблица 4 – Входные данные для расчёта рисков информационной безопасности для объекта 3 “Сервер, на котором хранятся БД ИСПДн, «ПАО Банк ЗенитБанк»”

Объект 3 : Сервер, на котором хранятся БД ИСПДн, «ПАО Банк ЗенитБанк»”		
Угроза/уязвимость	**Вероятность реализации угрозы через уязвимость в течении года %, P(V)**	**Критичность реализации угрозы через данную уязвимость %, ER**
Угроза 1 /Уязвимость 1	30	70
Угроза 1 /Уязвимость 2	40	70
Угроза 2 /Уязвимость 1	35	50
Угроза 2 /Уязвимость 2	35	60
Угроза 3 /Уязвимость 1	30	30
Угроза 3 /Уязвимость 2	45	50
Угроза 4 /Уязвимость 1	25	40
Угроза 4 /Уязвимость 2	40	60
Угроза 5 /Уязвимость 1	45	55
Угроза 5 /Уязвимость 2	50	50

После ввода входных данных произведем Расчет уровней угрозы по каждой уязвимости (Th) и по всем уязвимостям (CTh) для каждого ресурса ИС.
Расчетные данные для каждого объекта ИСПДн ПАО “ЗенитБанк” отображены в таблицах 5,6 и 7.

Таблица 5 – Итоги расчёта показателей Th, CTh для объекта 1 ИСПДн ПАО ЗенитБанк»

Угроза/уязвимость	**Уровень угрозы по каждой уязвимости %, Th** $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
Угроза 1 /Уязвимость 1	0,12	0,586
Угроза 1 /Уязвимость 2	0,53	
Угроза 2 /Уязвимость 1	0,09	0,245
Угроза 2 /Уязвимость 2	0,17	
Угроза 3 /Уязвимость 1	0,33	0,444
Угроза 3 /Уязвимость 2	0,17	
Угроза 4 /Уязвимость 1	0,13	0,278
Угроза 4 /Уязвимость 2	0,17	
Угроза 5 /Уязвимость 1	0,03	0,146
Угроза 5 /Уязвимость 2	0,12	

Таблица 6 – Итоги расчёта показателей Th, CTh для объекта 2 ЛВС, в рамках которой работники обеспечивают обмен информацией

Угроза/уязвимость	**Уровень угрозы по каждой уязвимости %, Th** $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
Угроза 1 /Уязвимость 1	0,32	0,754
Угроза 1 /Уязвимость 2	0,59	
Угроза 2 /Уязвимость 1	0,05	0,079
Угроза 2 /Уязвимость 2	0,07	
Угроза 3 /Уязвимость 1	0,03	0,109
Угроза 3 /Уязвимость 2	0,08	
Угроза 4 /Уязвимость 1	0,15	0,371
Угроза 4 /Уязвимость 2	0,26	
Угроза 5 /Уязвимость 1	0,12	0,190
Угроза 5 /Уязвимость 2	0,08	

Таблица 7 – Итоги расчёта показателей Th, CTh для объекта 3 Сервер, на котором хранятся БД ИСПДн, «ПАО Банк ЗенитБанк

Угроза/уязвимость	**Уровень угрозы по каждой уязвимости %, Th** $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$
Угроза 1 /Уязвимость 1	0,21	0,431
Угроза 1 /Уязвимость 2	0,28	
Угроза 2 /Уязвимость 1	0,18	0,352
Угроза 2 /Уязвимость 2	0,21	
Угроза 3 /Уязвимость 1	0,09	0,290
Угроза 3 /Уязвимость 2	0,22	
Угроза 4 /Уязвимость 1	0,1	0,316
Угроза 4 /Уязвимость 2	0,24	
Угроза 5 /Уязвимость 1	0,25	0,438
Угроза 5 /Уязвимость 2	0,25	

После расчета уровней угрозы по каждой уязвимости (Th) и по всем уязвимостям (CTh) для каждого ресурса ИС произведем расчет общего уровня угроз (CThR) действующего на объект и Расчет итогового риска по ресурсу (R) для каждого объекта ИСПДн ПАО Банка “ЗенитБанк”

Расчетные данные для каждого объекта ИСПДн ПАО “ЗенитБанк” отображены в таблицах 8,9 и 10.

Таблица 8 – Итоги расчёта показателя CThR для объекта 1 ИСПДн ПАО “ЗенитБанк”

Угроза/уязвимость	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - Th)$	**Общий уровень угроз по ресурсу %, CThR** $CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i)$	**Риск по ресурсу у.е., R**
Угроза 1 /Уязвимость 1	0,586	0,8928	89,28
Угроза 1 /Уязвимость 2			
Угроза 2 /Уязвимость 1	0,245		
Угроза 2 /Уязвимость 2			
Угроза 3 /Уязвимость 1	0,444		
Угроза 3 /Уязвимость 2			
Угроза 4 /Уязвимость 1	0,278		
Угроза 4 /Уязвимость 2			
Угроза 5 /Уязвимость 1	0,146		
Угроза 5 /Уязвимость 2			

Таблица 9 – Итоги расчёта показателя CThR для объекта 2 ЛВС, в рамках которой работники обеспечивают обмен информацией

Угроза/уязвимость	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$	**Общий уровень угроз по ресурсу %, CThR** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i)$	**Риск по ресурсу у.е., R**
Угроза 1 /Уязвимость 1	0,754	0,8971	89,71
Угроза 1 /Уязвимость 2			
Угроза 2 /Уязвимость 1	0,079		
Угроза 2 /Уязвимость 2			
Угроза 3 /Уязвимость 1	0,109		
Угроза 3 /Уязвимость 2			
Угроза 4 /Уязвимость 1	0,371		
Угроза 4 /Уязвимость 2			
Угроза 5 /Уязвимость 1	0,190		
Угроза 5 /Уязвимость 2			

Таблица 10 – Итоги расчёта показателя CThR для объекта 3 Сервер, на котором хранятся БД ИСПДн, ПАО Банк “ЗенитБанк”

Угроза/уязвимость	**Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$	**Общий уровень угроз по ресурсу %, CThR** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i)$	**Риск по ресурсу у.е., R**
Угроза 1 /Уязвимость 1	0,431	0,8583	85,83
Угроза 1 /Уязвимость 2			
Угроза 2 /Уязвимость 1	0,352		
Угроза 2 /Уязвимость 2			
Угроза 3 /Уязвимость 1	0,290		
Угроза 3 /Уязвимость 2			
Угроза 4 /Уязвимость 1	0,316		
Угроза 4 /Уязвимость 2			
Угроза 5 /Уязвимость 1	0,438		
Угроза 5 /Уязвимость 2			

Таким образом, в результате расчётов риск по ресурсам **(CR) равен 264,38 условных единиц.**

4. Рекомендации по улучшению мер защиты объекта ИСПДн

Оценка и обновление стратегий защиты персональных данных является важным этапом для минимизации рисков и обеспечения надежной защиты информационных активов. Далее представлены ключевые рекомендации, направленные на повышение уровня безопасности объекта ИСПДн и обеспечение надежной защиты персональных данных:

1. Применить сильное шифрования для защиты хранящихся и передаваемых данных.
2. Внедрить многофакторной аутентификации для повышения безопасности доступа к системе и защиты от несанкционированного доступа.
3. Реализовать строгого управления доступом с использованием принципов наименьших привилегий.
4. Регулярное обновлять программного обеспечения и операционных систем с применением последних патчей безопасности для устранения известных уязвимостей.
5. Регулярно развивать системы мониторинга и обнаружения инцидентов для постоянного отслеживания сетевой активности и выявления подозрительных действий.
6. Проводить регулярные аудиты безопасности для выявления и устранения потенциальных слабых мест в системе, а также для проверки соответствия стандартам безопасности.
7. Проработать защиту периметра сети с использованием брандмауэров, систем предотвращения вторжений и других средств безопасности для предотвращения несанкционированного доступа.
8. Регулярно создавать резервные копии данных и разработать план восстановления после инцидента (DRP) для минимизации потерь данных и снижения времени восстановления в случае инцидента.
9. Регулярно обучать сотрудников по вопросам кибербезопасности, включая осведомленность о социальной инженерии, фишинге и безопасном обращении с данными.

ЗАКЛЮЧЕНИЕ

В данном практической работе мы проверили успешно провели расчет рисков в ИСПДн Банка ПАО “ЗенитБанк”. Рассчитали такие показатели как уровень угрозы по каждой уязвимости, уровень угрозы по всем уязвимостям, через которые она может быть реализована, Общий уровень угроз по ресурсу и риск по ресурсу.

Выявили, что в результате расчётов риск по ресурсам равен 264,38 условных единиц. Важно отметить, что вероятность осуществления данных угроз для выбранных ресурсов также является очень высокой.

Полученная информация свидетельствует об скорейшем улучшения мер защиты объектов, связанных с информацией.