Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет безопасности информационных технологий

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

«Деловая игра по информационной безопасности»

Выполнил:

студент группы N3246,

Суханкулиев Мухаммет

(подпись)

Проверила:

Коржук Виктория Михайловна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – написать сценарий для игры-квеста на тему информационной безопасности. Цель игры – минимизировать ущерб, принимая "правильные" решения, используя знания о функциях защиты и классах защиты.

Для достижения поставленной цели необходимо решить следующие задачи:

– Описать компанию и роли в команде;

– Описать сценарий этапов и варианты решений, которые доступны ролям на том или ином этапе с указанием количества баллов за то или иное решение;

– Описать исходы при выборе решения с максимальным количеством баллов и со средним.

1 ДЕЛОВАЯ ИГРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Общие сведения о компании

Группировка «Свобода» занимается изучением аномальных явлений в Чернобыльской зоне, собирая уникальные данные о поведении аномалий, безопасных маршрутах и скрытых артефактах. В условиях постоянного противостояния с «Долгом» и военной угрозой информационная безопасность стала критически важной.

1.1.1 Роли в команде

1. **Специалист по защите данных** (отвечает за идентификацию источника утечки и настраивает защитные механизмы для предотвращения дальнейших угроз); далее – Спец. по ЗД
2. **Аналитик угроз** (оценивает риски, связанные с утечкой, а также предлагает возможные меры для минимизации ущерба); далее – Аналитик
3. **Специалист по внутреннему контролю** (проверяет доступ сотрудников к данным и выявляет слабые места в текущих мерах безопасности); далее – Спец. по ВК
4. **Руководитель по информационной безопасности** (принимает финальные решения, и разрабатывает стратегию защиты информации и восстановления систем). далее – Руководитель

1.2 Этапы события

1.2.1 Начальный этап – Диагностика

В «Свободе» фиксируется подозрительная активность в сети, замедление систем и частичная недоступность данных. Группировка подозревает утечку информации, но неясны ни масштаб, ни источник инцидента.

Спец. по ЗД	Аналитик	Спец. по ВК	Руководитель	Количество баллов
Мониторинг подозрительных IP-адресов и закрытие внешних соединений	Оценка потенциальных источников угроз и проверка доступных уязвимостей	Проверка доступа сотрудников к файлам и поиск аномалий в их действиях	Организовать оперативное совещание для сбора информации и координации действий	10
Беглый анализ логов сети	Составление списка подозрительных активностей за последние 24 часа	Блокировка доступа к конфиденциальным данным временно для всех сотрудников	Отправить оповещение об инциденте в общий чат сотрудников	5
Перезагрузка сервера без анализа логов	Не предпринимать никаких действий	Не проводить расследование среди сотрудников	Ожидание подтверждения инцидента	0
Исходы				
Максимальный балл (10)	Группировка «Свобода» успешно обнаружила и блокировала угрозы, сохранив критические данные и репутацию, что укрепило их позиции в зоне. – Защита обеспечена			
Средний/Минимальный балл (0-5)	Инцидент выявлен частично, но часть информации уже утекла, может подорвать доверие к «Свободе» среди других группировок, угрожая их исследовательской деятельности. – Продолжение игры			

1.2.2 Промежуточный этап 1 – Анализ угрозы

Доступ злоумышленника подтверждён. Группировке необходимо понять, какие данные были скомпрометированы и оценить возможный ущерб.

Спец. по ЗД	Аналитик	Спец. по ВК	Руководитель	Количество баллов
Изучение данных, к которым получен несанкционированный доступ	Оценка возможных внешних угроз, которые могли использовать текущие уязвимости	Провести расследование среди сотрудников, имеющих доступ к критически важной информации	Утверждение стратегии по устранению угрозы, основанную на анализе предыдущих специалистов	10
Общее сканирование уязвимостей системы	Консультация с внешними экспертами	Сосредоточиться на действиях одного подозрительного сотрудника.	Консультация с менеджером	5
Запланировать анализ на неопределённое время	Ожидать, что угрозу минует сама по себе	Не участвовать в анализе	Дождаться новых данных для принятия решений	0
Исходы				
Максимальный балл (15-20)	Команда собрала достаточно информации о злонамеренных действиях, предотвратив катастрофические потери и сохранив важные артефакты. – Защита обеспечена			
Средний/Минимальный балл (0-10)	Некоторые аспекты остаются под угрозой, что может привести к новым атакам со стороны «Долга» или военных. – Продолжение игры			

1.2.3 Промежуточный этап 2 – Меры по восстановлению

Для защиты данных и предотвращения дальнейших утечек группировка должна быстро реализовать меры по восстановлению системы и устранению уязвимостей.

Спец. по ЗД	Аналитик	Спец. по ВК	Руководитель	Количество баллов
Перенастройка ключевых систем безопасности, включая шифрование критичных данных, и устранение выявленных уязвимости	Проведение оценки всех потенциальных рисков после инцидента и составление плана для дальнейшего восстановления	Введение строгих проверок доступа к данным на период восстановления и проведение внепланового аудита привилегий	Организовать постоянный мониторинг сетевой активности для быстрого реагирования на возможные угрозы	10
Временное ограничивание доступа к наиболее важной информации и/или внедрение двухфакторной аутентификации	Определение только основных уязвимостей, которые могли быть использованы	Отключение доступа сотрудникам без проверки привилегий	Поручить команде дополнительные проверки без запуска постоянного мониторинга	5
Игнорировать необходимость в изменениях	Полагаться на имеющиеся системы защиты, предполагая, что они сработают в следующий раз	Не вносить никаких изменений в текущий контроль доступа	Решить, что ситуация уже стабилизирована, и завершить все действия по восстановлению	0
Исходы				
Максимальный балл (20-30)	«Свобода» быстро восстановила системы, увеличив защиту данных, и тем самым укрепила свою защиту от будущих инцидентов. – Защита обеспечена			
Средний/Минимальный балл (0-15)	Группировка контролирует ситуацию, но некоторые уязвимости остаются, что может привлечь внимание «Долга» или военных. – Продолжение игры			

1.2.4 Промежуточный этап 3 – Обеспечение будущей защиты

После устранения текущих проблем требуется внедрить новые меры и стратегии для предотвращения подобных инцидентов в будущем, чтобы усилить безопасность группировки.

Спец. по ЗД	Аналитик	Спец. по ВК	Руководитель	Количество баллов
Внедрение обновлённых политик шифрования и частых проверок на уязвимости	Составление подробного отчёта о текущих угрозах и разработка рекомендаций для усиления всех слабых мест	Пересмотреть систему привилегий, усилить контроль над доступом к критически важной информации	Создание долгосрочной стратегии кибербезопасности и запуск обучения сотрудников по защите данных	10
Настройка регулярных проверок на уязвимости, но без обязательного обновления политики	Создание общего плана противодействия угрозам, но без конкретных рекомендаций по уязвимостям	Установить временные ограничения доступа к важным данным	Провести одноразовое обучение сотрудников и информирование их об основных правилах безопасности	5
Не предпринимать дополнительные действия	Не предпринимать дополнительные меры	Не вносить изменения	Не организовывать дополнительные мероприятия	0
Исходы				
Максимальный балл (25-40)	«Свобода» усилила свою безопасность, что значительно снизило риски новых инцидентов и укрепило позиции в зоне. – Защита обеспечена			
Средний/Минимальный балл (0-20)	Хоть группировка предприняла важные шаги для защиты, некоторые риски остались неустранёнными. – Продолжение игры			

1.2.5 Заключительный этап – Подведение итогов

Оценка проделанной работы, анализ эффективности принятых решений и определение итогового уровня ущерба.

Спец. по ЗД	Аналитик	Спец. по ВК	Руководитель	Количество баллов
Детализированный отчёт по выполненным мерам и предложения возможных улучшений	Анализ всего инцидента, выявление дополнительных угроз и предоставление плана для будущих действий	Проверка правильности выполнения всех мер, связанных с доступом, и выявление оставшихся пробелов	Сделать презентацию для команды и менеджмента, описывая итоги и дальнейшие шаги по усилению безопасности	10
Краткий отчёт о проведённых действиях	Оценка инцидента в целом, но без предложений по дополнительному улучшения	Проверка только для одного аспекта контроля доступа	Сделать краткую презентацию итогов	5
Не участвовать в подготовке итогового отчёта	Не участвовать в анализе	Не проводить проверки	Не делать презентацию	0

1.3 Итоговые события

Максимальный балл (40-50) – Защита обеспечена: Группировка «Свобода» успешно восстановила все утраченные данные и разработала эффективную стратегию защиты. Успешные действия укрепили их репутацию и позиции в зоне, что позволило продолжать исследования и взаимодействие с другими группировками без потери доверия. Все угрозы были нейтрализованы, и группа готова к будущим вызовам.

Средний балл (25-35) – Защита нарушена: Ущерб удалось снизить, но некоторые уязвимости остались неустранёнными. Это может подорвать доверие к «Свободе» среди других группировок, и они могут столкнуться с новыми угрозами, исходящими от «Долга» или военных. Группировка должна продолжать работу над улучшением безопасности и восстановлением утраченного доверия, что может потребовать дополнительных ресурсов и времени.

Минимальный балл (0-20) – Защита разрушена: Группировка может столкнуться с активными атаками со стороны «Долга», что угрожает не только их исследовательской деятельности, но и безопасности всех членов команды. Восстановление после такого инцидента потребует значительных усилий и ресурсов, и группа может потерять доступ к ключевым артефактам и данным.

ЗАКЛЮЧЕНИЕ

Я разработал сценарий игры-квеста по информационной безопасности, направленной на минимизацию ущерба от инцидентов. Применение методов защиты и оценки решений позволило создать эффективные сценарии реагирования на угрозы.

Полученные навыки помогут мне в будущем для улучшения стратегий обеспечения безопасности данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ТИБиМЗИ – Лекция 4 – https://drive.google.com/file/d/1vPBza4M_pBLn5Aqcs4CNWfpfmA81VWus/view?usp=drive_link
2. ЛР4 – Деловая игра по ИБ – https://docs.google.com/document/d/1INtaqfxBjD0K8x6CiQ16uN7r-bWCaohj/edit?usp=drive_link&ouid=106732121730871930798&rtpof=true&sd=true