Слайд 1 (Титульный)

Здравствуйте уважаемые слушатели. Представляю вам доклад на тему ПОДХОД К ОРГАНИЗАЦИИ АУДИТА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.

Слайд 2 (Актуальность исследования)

Обеспечение безопасности корпоративной информационной системы в настоящее время является актуальной проблемой. Согласно данным предоставленным МВД, только за январь-июнь 2020г. рост IT-преступности в России составил 91,7% по сравнению с аналогичным периодом прошлого года. А к концу года число прогнозируемых зарегистрированных киберпреступлений составляет около 0,5 млн. На представленном слайде вы могли ознакомиться с динамикой IT-преступлений за последние 7 лет.

Слайд 3 (Предметная область)

Предметной областью исследования является система менеджмента информационной безопасности. В работе используются требования стандарта ISO/IES27001 для проведения аудита. Вообще, данный стандарт предназначен для применения организациями любой формы собственности. Так же устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности среди общих бизнес-рисков организации.

Слайд 4 (Цель исследования; Задачи исследования)

Проведение аудита информационной безопасности нацелено на поиск уязвимостей системы, через которые может быть реализован ее взлом. Законность проводимого при аудите взлома подтверждается письменно до начала проведения. Аудит информационной безопасности можно разделить на 3 этапа: разработка регламента проведения аудита, сбор информации об исследуемой ИС, составление отчета уровня безопасности.

В данной работе упор был сделан непосредственно на сбор информации об исследуемой ИС. Данный этап условно делится на 4 шага, которые и являются задачами исследования, и представлены на слайде.

Слайд 5 (Научная новизна)

Научная новизна работы заключается в разработке моделей представления знаний и средств обеспечения информационной безопасности в корпоративной сети компании, направленных на управление рисками информационной безопасности. Разработана модель благодаря которой можно собрать данные об уязвимостях и сформировать из этих данных базу знаний, в которой указываются проблемы существующего решения и возможности её решениия, чтобы при последующих аудитах использовать накопленнный опыт. Что соотетсвует стандарту ISO и облегчает оценку и обработтку рисков, а также внедрение защитных мер. Так же в бз постоянно будут добавляться информацио о новых уязвимостях. Рассмотрим первые 3 шага по-отдельности.

Слайд 6 (Пассивный сбор информации)

Для пассивного сбора информации следует использовать набор запросов для выявления уязвимостей в системе безопасности Google Dork. Благодаря GDQ можно найти файлы и извлечь из них полезную для взлома информацию.

Слайд 7 (Активный сбор информации)

Далее выполняется активный сбор информации об исследуемом объекте. Во время активного сбора информации происходит непосредственное взаимодействие с исследуемым объектом. При этом используются сканеры уязвимостей, специальные утилиты и фреймворки. Рекомендуется использовать такие сканеры: Wapiti3, Sqlmap, Acunetix WVS, Vega.

Слайд 8 (Сканирование сети)

Для сканирования сети используют утилиты: whois, nslookup, recon-ng. Они позволяют по доменному имени определить IP-адрес, а также узнать диапазон сети. Помимо информации о сети на шаге сканирования сети предпринимаются действия по выявление уязвимостей, позволяющих получить контактные данные сотрудников. Так же на данном шаге используются методы социальной инженерии, такие как использование фишинговых сайтов, email-редирект. Проверка компетентности работников позволяет установить их уровень образованности в данной сфере, что необходимо для разработки эффективной стратегии обучения персонала.

Слайд 9 (Результаты)

В результате проделанной работы была разработана методика, которая рекомендуется к использованию при проведении аудита информационной безопасности. Полученная информация в процессе проведения аудита послужит основой для создания базы знаний, которая позволит при последующих аудитах повторно использовать рекомендации эксперта в области информационной безопасности в случае обнаружения уязвимостей в системе.