Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:658.52

НАВАЦКАЯ
Елена Андреевна

Система обеспечения информационной безопасности промышленного предприятия

Автореферат
на соискание степени магистра
по специальности 1–98 80 01 Информационная безопасность

_____

Научный руководитель
Заведующий кафедрой защиты
информации, д.т.н., профессор
БОРБОТЬКО Тимофей
Валентинович

_____

Минск 2023

ВВЕДЕНИЕ

Развитие компьютерных и интернет-технологий изменило жизнь людей и коренным образом изменило способ ведения бизнеса организациями. Вместе с тем, развитие технологий и цифровизация вызывали рост преступных действий нарушителей. Растущая угроза атак на критическую инфраструктуру, дата-центры, а также на частный/общественный, оборонный, энергетический, государственный и финансовый секторы бросает вызов каждому, начиная от отдельного человека и заканчивая крупными корпорациями. Целью этих атак являются финансовые кражи, шпионаж, саботаж, кража данных и интеллектуальной собственности, что приводит к различным последствиям, начиная от незначительных утечек данных и заканчивая крупными материальными и репутационными потерями.

По мере того, как растут навыки и аппетиты нарушителей, развивается и сфера ИБ. Постоянное совершенствование знаний и навыков специалистов ИБ, обнаружение несанкционированных вторжений и реагирование на них имеет решающее значение в борьбе с нарушителями.

В целях защиты от угроз ИБ применяется комплекс организационно-технических мер, направленный, в первую очередь, на предотвращение несанкционированного доступа нарушителя в ИС организации, а также на выявление, расследование и минимизацию последствий от инцидента ИБ.

Целью диссертационной работы является создание системы обеспечения информационной безопасности промышленного предприятия.

Для достижения поставленной цели в диссертации необходимо решить следующие задачи:

— проанализировать модель нарушителя, целью которого является промышленный шпионаж, согласно методологии MITRE ATTACK;

— проанализировать ИС предприятия и сформировать исходные данные;

— разработать СЗИ для ИС предприятия;

— проверить созданную СЗИ предприятия.

Создание системы обеспечения информационной безопасности позволит обеспечить защиту от несанкционированных действий сторонних нарушителей, а также повысить контроль за действиями работников предприятия.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в создании системы обеспечения информационной безопасности промышленного предприятия.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать модель нарушителя, целью которого является промышленный шпионаж.
2. Проанализировать информационную систему предприятия.
3. Разработать систему защиты информации для информационной системы предприятия.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XIX Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2023).

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 печатная работа, в том числе 1 статья и тезис в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из общей характеристики работы, перечня условных обозначений, введения, трех глав, заключения, библиографического списка.

Общий объем диссертационной работы составляет 71 страницу, из них 54 страницы текста, 17 рисунков на 17 страницах, 1 таблица на 1 странице, список использованных библиографических источников (16 наименований), список публикаций автора по теме диссертации (1 наименование) на 1 странице и 1 приложение на 1 странице.

Проверка на уникальность

Проведена экспертиза диссертации Навацкой Е.А. «Система обеспечения информационной безопасности промышленного предприятия» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиатплюс» (адрес доступа: https://antiplagius.ru/) в on-line режиме 14.06.2023 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 88,90 %). Отчет о результатах проверки представлен в Приложении А.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрены современные проблемы развития компьютерных и интернет-технологий, вместе с которыми растет угроза атак на ИС предприятий.

В общей характеристике работы показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе магистерской диссертации рассмотрена методология MITRE ATT&CK в описании модели нарушителя, целью которого является промышленный шпионаж. Приведено сравнение двух моделей последовательности тактик атак – Cyber Kill Chain и база знаний MITRE ATT&CK. Создана тепловая карта наиболее часто использующихся техник MITRE ATT&CK, которые используют нарушители, целью которых является промышленный шпионаж.

Во второй главе сформированы исходны данные, необходимые для построения системы обеспечения инфорационной безопасности на предприятии, на основе наиболее часто используемых техник и подтехник, которые успешно использовались при имитации реальной атаки нарушителя. Также определены методы обнаружения и противодействие несанкционированным действиям нарушителей.

В третьей главе определен и проанализирован объект защиты информации – ERP-система. Определены основные характеристики система

мониторинга событий ИБ предприятия, необходимые для поддержания ИБ на должном уровне. Установлены требования для парольной политики, а также настроены необходимые параметры безопасности серверов.

Создана методика реагирования на выявленные специалистами ИБ инциденты ИБ. На примере атаки нарушителя, конечной целью которого является промышленный шпионаж, протестирована работа созданной системы обеспечения ИБ и отработаны действия специалистов ИБ по реагированию на выявленную атаку, на примере матрицы MITRE ATT&CK.

ЗАКЛЮЧЕНИЕ

На основе анализа методологии MITRE ATT&CK была сформирована усредненная модель нарушителя, целью которого является промышленный шпионаж, а также построена тепловая карта с наиболее часто использующимися нарушителями техниками.

На основе анализа ИС предприятия сформированы общие исходные данные, основанные на анализе наиболее часто используемых техник и подтехник, которые успешно использовались при имитации реальной атаки нарушителя. Также определены методы обнаружения и противодействие несанкционированным действиям нарушителей.

Определен и проанализирован объект защиты информации – ERP-система. Определены основные характеристики система мониторинга событий ИБ предприятия, необходимые для поддержания ИБ на должном уровне. Установлены требования для парольной политики, а также настроены необходимые параметры безопасности серверов.

Создана методика реагирования на выявленные специалистами ИБ инциденты ИБ. На примере атаки нарушителя, конечной целью которого является промышленный шпионаж, протестирована работа созданной системы обеспечения ИБ и отработаны действия специалистов ИБ по реагированию на выявленную атаку, на примере матрицы MITRE ATT&CK.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

Навацкая, Е. А. СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОЛОГИЙ CYBER KILL CHAIN и MITRE ATT&CK / Навацкая Е.А. // Управление информационными ресурсами: материалы XIX Международной научно-практической конференции, Минск, 22 марта 2023 г.; Академия управления при Президенте Республики Беларусь. / под ред. Т.В. Борботько – Минск,

Академия управления при Президенте Республики Беларусь, 2022. – С. 248-249.