Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2020 г.

Разработка методики проведения компьютерно-технических экспертиз при расследовании инцидентов информационной безопасности в автоматизированных системах

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2020.151.ПЗ ВКР

Руководитель проекта,
Начальник отдела АНО «Центр экспертиз и научно-технических исследований»
_____ В.С. Лужнов
_____ 2020 г.

Автор проекта,
студент группы КЭ-407
_____ Д.Е. Карманов
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Карманов Д.Е. Разработка методики проведения компьютерно-технических экспертиз при расследовании инцидентов информационной безопасности в автоматизированных системах – Челябинск: ЮУрГУ, КЭ-407, 48 с., библиогр. список – 59 наим.

Выпускная квалификационная работа выполнена с целью разработки методики проведения компьютерно-технических экспертиз для расследования инцидентов информационной безопасности.

В выпускной квалификационной работе отражены все этапы проведения экспертизы при расследовании инцидентов информационной безопасности, от сбора исходных данных до заключения в соответствии нормативным документам РФ по защите персональных данных.

В процессе выполнения квалификационной работы была разработана методика проведения компьютерно-технической экспертизы, проведено сравнение существующих нормативных документов, регламентирующих систему управления инцидентами информационной безопасности, приведены все необходимые документы, регламентирующие порядок проведения экспертизы.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ 7
ВВЕДЕНИЕ 8
1 ТЕОРЕТИЧЕСКОЕ ОПИСАНИЕ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 9
1.1 Определение инцидента информационной безопасности 9
1.2 Обзор существующих практик по управлению инцидентами 12
1.3 Реагирование на инциденты информационной безопасности 13
1.3.1 Цели процесса реагирования на инцидент 13
1.3.2 Основные этапы процесса реагирования на инциденты информационной безопасности 13
1.4 Расследование инцидента информационной безопасности 14
1.5 Выводы 17
2 КОМПЬЮТЕРНО-ТЕХНИЧЕСКИЕ ЭКСПЕРТИЗЫ 18
2.1 Определение судебной экспертизы 18
2.2 Определение компьютерно-технической экспертизы 19
2.3 Определение экспертной методики 20
2.4 Требования законодательства к методике (и методам) производства экспертизы 21
2.5 Анализ методик производства КТЭ 23
2.6 Выводы 25
3 МЕТОДИКА ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ 26
ЭКСПЕРТИЗЫ 26
3.1 Подготовительная стадия 26
3.2 Аналитическая стадия 30
3.3 Эксперимент 34
3.4 Синтезирующая стадия 35
3.5 Результативная стадия 40
3.6 Формирование выводов 40
3.7 Заключение эксперта 40
3.8 Оценка эффективности разработанной методики производства экспертизы 41
3.9 Выводы 43
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 44

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

ИБ – Информационная безопасность.
КТЭ – компьютерно-техническая экспертиза.
ОС – операционная система.
НЖМД – накопитель на жестком магнитном диске.
ПО – программное обеспечение.

ВВЕДЕНИЕ

С развитием информационных технологий меняется характер информационной безопасности и преступлений в информационных и компьютерных системах. Большинство инцидентов, связанных с нарушениями безопасности систем, считаются преступлениями. Можно выделить основные типы инцидентов: кража информации, несанкционированный доступ, промышленный шпионаж. Данные нарушения являются инцидентами, так как нарушаются законы. Защитные меры информационной безопасности или типовые политики по защите информации не могут полностью гарантировать защиту информационных систем, сетей или сервисов. Вероятно, что останутся уязвимые места после внедрения защитных мер, в связи с этим появляется угроза появления инцидентов информационной безопасности. Инциденты информационной безопасности могут оказывать негативное воздействие на бизнес организации. Кроме того, неизбежно будут возникать новые угрозы, которые ранее не были выявлены.

Исходя из вышеуказанного можно сказать, что данная проблема является актуальной на текущий момент. В связи с этим появляется необходимость в экспертных учреждениях и экспертах в методике, которая бы позволяла проводить расследования инцидентов и при этом гарантировала объективность и доказательную базу результатов КТЭ.

Целью данной выпускной квалификационной работы является разработка методики проведения КТЭ для расследования инцидентов информационной безопасности в автоматизированных системах.

Для достижения указанной цели необходимо решить следующие задачи:

- изучить задачи и порядок реагирования на инциденты ИБ;
- разработать методику проведения КТЭ в рамках расследования инцидентов ИБ и провести ее апробацию на конкретном объекте в рамках практической деятельности.