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

УДК 004.056:336.71.078.3

Рабцевич
Роман Владимирович

«Методика расследования компьютерно-технических преступлений в системах безналичных электронных платежей»

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель

Маликов Владимир Викторович
кандидат технических наук, доцент

Минск 2016

ВВЕДЕНИЕ

Необходимость разработки научно-обоснованной методической базы, способствующей повышению эффективности расследования компьютерно-технических преступлений в системах безналичных электронных платежей, связана с ростом числа высокотехнологичных киберпреступлений, а также значительными величинами финансовых потерь организаций различных форм собственности и граждан при атаках на такие системы со стороны преступников. Внедрение методики расследования компьютерно-технического преступления, основанная на построении и анализе модели преступления с учетом прогнозирования возможных вариантов локализации его последствий позволит сотрудникам служб безопасности проводить оперативное документирование фактов несанкционированного доступа для дальнейшей правой оценки следственными органами.

По оценкам экспертов в области информационной безопасности число киберпреступлений будет только расти, а несовершенные во многом методы расследования преступлений могут еще больше упростить задачу нарушителям ИБ.

В связи с этим, актуальным на сегодняшний день является вопрос повышения эффективности расследования компьютерно-технических преступлений в СБЭП.

Возникающие проблемы при обнаружении инцидентов безопасности можно решить только комплексным подходи и автоматизацией принимаемых мер. Первое и самое важное в начале расследования - скорость реакции. Чем быстрее офицеры безопасности начнут собирать данные об инциденте, чем скорее он будет зафиксирован, тем больше вероятность раскрытия.

Не менее важно получение и анализ данных должен, они должны проводиться с привлечением технических специалистов, а также программно-технических средств актуальных на момент проведения расследования.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Данная работа посвящена методике расследования компьютерно-технических преступлений в системах безналичных электронных платежей, представляющей практический интерес.

Объектом исследования является структура рынка киберпреступности, а также организационно-технические и технические решения для совер-шения преступлений со стороны криминальных организаторов.

Предметом исследования являются организационно-технические и технические методы и средства, способствующие повышению эффективности расследования компьютерно-технических преступлений в системах безналичных электронных платежей.

Основными задачами являются:

- построение модели/структуры рынка киберпреступности;
- определение основных схем/технологий, используемых преступниками;
- обоснование и выбор организационно-технических и технических методов и средств для повышения эффективности расследования компьютерно-технических преступлений.

Целью работы является разработка методики расследования компьютерно-технических преступлений в системах безналичных электронных платежей.

Для достижения данной цели необходимо решить следующие задачи:

- рассмотрение концептуальных основ построения систем защиты в СБЭП;
- разработка методических основ выбора и применения типовых методов и средств защиты;
- разработка подхода по оценке эффективности систем защиты в СБЭП, а также комплексных показателей и критериев оценки эффективности защиты;
- оценка применимости существующих подходов для повышения эффективности расследования преступлений в СБЭП.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи, формулируются основные положения диссертации, выносимые на защиту.

Первый раздел «Статистические данные по компьютерно-техническим преступлениям в системах безналичных электронных платежей» носит теоретический характер и состоит из двух подразделов.

В подразделе 1.1. «Угрозы безопасности в СБЭП» выделены два существенных вопроса. Первый – статистические данные по нарушению систем защиты. Анализ угроз, проведенных агентством национальной ассоциацией информационной безопасности в США выявил следующую статистику: 43%

угроз – сбои оборудования, 26% - неумелые или неправильные действия персонала, 15% - вредительские действия собственных сотрудников, 8% - внешние атаки по сети Интернет и 5% - воздействие компьютерных вирусов. Классификация угроз информационной безопасности является вторым вопросом и рассматривается в подразделе 1.1.2. Все источники угроз безопасности информации можно разделить на три основные группы: обусловленные действиями субъекта (антропогенные источники угроз); обусловленные техническими средствами (техногенные источники угрозы); обусловленные стихийными источниками.

В подразделе 1.2. «Статистические данные по методам и средствам обеспечения информационной безопасности в СБЭП» рассматриваются организационно-технические и технические средства защиты информации. Рассмотрены уровни защиты: законодательный, административный, процедурный и программно-технический. Приведены аппаратные и программные средства защиты информации.

Обзор существующих подходов по обеспечению расследования преступлений в СБЭП рассмотрены в подразделе 1.3. Описана необходимость и важность взаимодействия следователей с операторами связи и специалистами по безопасности. Приведены примеры методов и подходов по обеспечению расследования с помощью технических средств и специализированных программ.

Второй раздел «Оценка эффективности методов и средств защиты в СБЭП» состоит из трёх разделов, рассматривающих концептуальные основы построения систем защиты на основе (подраздел 2.1), методические основы выбора и применения типовых методов и средств защиты (подраздел 2.2), а также подраздел, посвященный разработке подхода по оценке эффективности систем защиты. В подразделе 2.1 рассмотрены подходы к практической реализации системы защиты информации. Первый подход состоит в разработке и внедрению новых информационно-вычислительных систем, в рамках которых решается весь комплекс проблем информационной безопасности. Второй подход состоит в разработке подсистем защиты информации, объединении их в единую систему защиты, налагаемую на уже созданную информационную систему, в которой изначально не предусматривался полный комплекс защитных механизмов.

В подразделе 2.3 приведены этапы построении комплексной системы защиты от утечек, рассмотрена модель нарушителя безопасности, разработаны критерии эффективности систем защиты.

Третий раздел «Разработка методики расследования компьютерно-технических преступлений в СБЭП» носит практико-ориентированный

характер и состоит из трёх подразделов, рассматривающих статистические данные по утечкам (подраздел 3.1), оценку применимости существующих подходов для повышения эффективности расследования преступлений в СБЭП (подраздел 3.2), а также включает разработку методики расследования преступлений (подраздел 3.3). В подразделе 3.2 рассмотрены способы защиты от наиболее распространённых способов воровства конфиденциальной информации: 1) физический доступ к местам ее хранения и обработки; 2) использование резервных копий; 3) несанкционированный доступ сотрудниками банка. В подразделе 3.3 рассмотрен пример модели преступления, а также возможные варианты решения. Основной проблемой при расследовании преступлений данного характера, является постоянное совершенствование технических и программных средств используемых преступниками, а также доказательство причастности конкретных правонарушителей. Крайне важно при расследовании преступлений в сфере СБЭП, руководствоваться четкими правилами и совершать последовательные действия согласно рекомендациям ведущих организаций в сфере расследования киберпреступлений.

В четвертом разделе «Автоматизация подходов по расследованию компьютерно-технических преступлений в СБЭП» даны рекомендации по методике расследования типичных инцидентов. Сделаны акценты на наиболее важных деталях и действиях проводимых при расследовании. Первое и самое важное в начале расследования - скорость реакции, привлечение технических специалистов, анализ цифровых данных и следов с помощью программных и программно-аппаратных средств. В подразделе 4.2 рассмотрено и проанализировано программное обеспечение по обеспечению расследования компьютерно-технических преступлений. Рассмотренные программные продукты и методы расследования однозначно ускоряют проведение экспертизы и избавляют сотрудников от ручного труда, в дальнейшем могут использоваться для предотвращения утечек информации.

ЗАКЛЮЧЕНИЕ

Базируясь на проведенных в диссертационной работе теоретических исследованиях, касающихся разработки методов расследования типовых инцидентов в системах безналичных электронных платежей, можно сделать вывод:

– проведен анализ статистических данных по компьютерно-техническим преступлениям в системах безналичных электронных платежей, на основе которого показана динамика их количественного и качественного роста, а также неэффективность применяемых организационно-технических и технических мер защиты.;

– обосновано, что главной задачей при организации расследования инцидента информационной безопасности является поиск источника утечки информации, а также правильно выбранная и регламентированная последовательность действий сотрудников, проводящих расследование таких инцидентов;

– установлено, что для эффективной защиты конфиденциальной информации в СБЭП необходимо совместное применение организационно-технических и технических методов.;

– при анализе этапов расследования компьютерно-технических преступлений для типовых инцидентов доказано, что оптимальным с точки зрения технических и организационно-правовых методов расследования является тесное сотрудничество следователей со специалистами по ИБ, четкая последовательность действий регламентируемая или рекомендованная ведущими агентствами по информационной безопасности. Описаны технические методы, рекомендованные к обязательному применению при таком расследовании.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Маликов, В.В. Исследование структуры и технологий совершения киберпреступлений / В.В. Маликов, Р.В. Рабцевич, С.В. Пузына // 50-лет МРТИ-БГУИР: материалы Международной НТК – Минск, 18-19 марта 2014 г. : в 24./БГУИР; редкол. : А.А. Кураев [и др.] – Мн., 2014. 4.1 – с.396-397

2-А. Маликов В.В. Исследование технологий совершения компьютерно-технических преступлений в системах безналичных электронных платежей / В.В. Маликов, Р. В. Рабцевич, С. В. Пузына // Теоретические и прикладные аспекты информационной безопасности: материалы междунар. НПК, Минск, 19 июня 2014 г./ Мн.: Акад. МВД, 2015. – С. 163 – 166.