ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента Баранковой Инны Ильиничны на диссертационную работу Макаровой Ольги Сергеевны на тему «Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы исследования

Защита информации (ЗИ) предусмотрена Статьей 16 Федерального закона (ФЗ) от 27.07.2006 «Об информации, информационных технологиях и о защите информации», а также иными нормативно-правовыми актами, разработанными государственными регуляторами в области информационной безопасности (ИБ), в том числе, в сфере защиты критической информационной инфраструктуры. При этом действующим законодательством предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми.

В этой связи разработка новых методов оценки угроз ИБ является актуальной задачей.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научные результаты:

научно обоснована математическая модель оценки вероятности реализации нарушителем компьютерной атаки (КА) и идентификации ее параметров, основанная на положениях Теории положений криминологии (ТПК);

научно обоснована математическая модель, описывающая динамику возможности реализации нарушителем компьютерной атаки во времени, основанная на положениях Теории диффузии инноваций (ТДИ), и идентифицированы ее параметры;

научно обоснована методика прогнозирования динамики векторов КА, построенная с точки зрения нарушителя КА.

Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов исследования базируется на использовании известных математических методов, адекватных задачам исследования, а также согласованностью оценок КА, полученных с помощью предложенных моделей и

методики, с результатами анализа известных КА и результатами натурного моделирования КА, проведенного с помощью ПАК «Ampire»

Результаты исследования опубликованы в 10 научных работах, 6 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом УрФУ, включая 2 в изданиях, индексируемых в международных цитатно-аналитических базах данных.

Практическая значимость результатов диссертации

Разработана методика прогнозирования динамики векторов КА с точки зрения нарушителя, позволяющая выявлять тренды развития КА. Полученные результаты внедрены в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», (Екатеринбург, Россия); в Акционерном обществе «Перспективный мониторинг», (Москва, Россия).

Оценка содержания диссертации и её оформления

Диссертационная работа содержит 179 страниц основного текста (всего 218 с.), 26 рисунков (без приложений) и 25 таблиц (без приложений). Она состоит из введения, трех глав, заключения, списка сокращений, списка литературы из 178 наименований, 8 приложений.

В первой главе проведен анализ предметной области, в том числе анализ нормативно-правовых документов РФ и международных стандартов, по оценке угроз и рисков ИБ, анализ основных научных подходов в области оценки угроз ИБ. На основании результатов анализа состояния предметной области сформулированы цель и задачи исследования.

Во второй главе проведена разработка и обоснование принципов и подходов к построению и разработке математических моделей, описывающих принятие решения нарушителем о проведении КА и динамику распространения КА. В качестве таковых выбраны: теория принятия решений, общая практика выявления и предупреждения правонарушений, ИТ-подходы к выявлению уязвимостей, ТПК.

В третьей главе проведен анализ общедоступных источников информации о КА, в частности, отчеты производителей средств ЗИ, данные из DarkNet, отчеты центров мониторинга инцидентов ИБ и новостных агрегаторов. Сделаны обоснованные выводы о возможности использования указанных источников.

Разработана и проведена апробация методики прогнозирования вектора КА. Представлено практическое применение методики при прогнозировании вектора целевых и нецелевых КА, полученное на основе использования информации о более чем 700 тысячах обнаруженных КА

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по содержанию диссертации:

1. Подтверждение адекватности методики прогнозирования динамики векторов КА (п.4 Практическая и теоретическая значимость) не может являться практической значимостью, практической значимостью является разработка методики.
2. В первой главе при описании существующих методик автор указывает, что действующая нормативно-правовая документация не предусматривает учет наиболее вероятных векторов КА. Такой учет может производится при дополнении адаптированного уточнённого базового набора мер защиты информации.
3. Автор делает неправильный вывод об одновременном применении к одной и той же системе всех возможных нормативно-правовых документов (с.30 диссертации «для значимых объектов КИИ, являющихся ИСПД необходимо учитывать Требования к защите ПД при их обработке в ИСПД»). Информационные системы значимых объектов КИИ выделяются в отдельные контуры без доступа в корпоративную сеть предприятия и никак не могут быть связаны с ИСПДн. К каждой системе будут применяться свои требования
4. Анализ поведения нарушителя проводится с точки зрения только внешнего нарушителя, хотя наибольший ущерб приносят внутренние нарушители. Можно ли адаптировать предложенную методику для этой категории?
5. Проводилась ли количественная оценка влияния на защищенность информации и расходование ресурсов учет позиции нарушителя?
6. Каким образом в математической модели учитываются «идейные» мотивы нарушителя, например, от «обиженных» сотрудников
7. Какой смысл имеет коэффициент b и как обосновывается его значение равное единице в формуле 2.12
8. В каком диапазоне выбирается коэффициент имитации (формула 2.14)?
9. По приведенным рис.2.2 и рис.2.3 нельзя сделать однозначный вывод о влиянии параметров p и q на функции S(T) и Y(T). Что оказывает большее влияние параметр p, q или эффект взаимодействия?

10. Автор указывает, что для нахождения решения задач (2.23), (2.24) на. 97 использовалась функция пакета MATLAD (не существует), на с.108 указан пакет МАТДАD (не существует) и пакет MATCAD. Какой пакет был использован?
11. В итогах анализа математической модели развития компьютерной атаки сказано, что «не зависит от внешних характеристик, в частности, экономичности и рентабельности реализации метода КА, наличием рекламы в DarkNet и данными межличностного взаимодействия нарушителей и апробации (совместимости с инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА» Следует ли из этого что указанные параметры могут быть исключены из модели? При расчете параметров возможности реализации метода КА они используются.

Сделанные замечания не снижают научной ценности работы.

Заключение по работе

Исследовательская работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, личному вкладу автора, отражению результатов в публикациях, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автор диссертации Макарова Ольга Сергеевна заслуживает присуждения ей учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Доктор технических наук, доцент
Заведующая кафедрой информатики и информационной безопасности
Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова»
Тел.: +7 (3519) 23-27-51
e-mail: inna_barankova@mail.ru
Адрес: 455000, г. Магнитогорск, пр. Ленина, д.38, УК 1, ауд. 368

Личную подпись заверяю
Начальник отдела кадров
ФГБОУ ВО «МГТУ им. Г.И. Носова»
«06» 12 2021

6.12.21

Баранкова Инна Ильинична