Экз № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента Козачка Александра Васильевича 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

Тема оценки угроз информационной безопасности (ИБ) является актуальной, в том числе и в свете, появившихся в 2017 году требований по защите критической информационной инфраструктуры. В соответствии с «Методикой оценки угроз безопасности информации», разработанной ФСТЭК России, оценка угроз ИБ осуществляется на основе экспертных оценок. Международные стандарты в области защиты информации рекомендуют использовать те или иные известные методологии, каждая из которых, де-факто, базируются на предопределенном наборе мер защиты информации (ЗИ) в зависимости от категории информационной системы, либо на оценке рисков ИБ для которой свойственен экспертный метод.

Необходимо отметить, что метод экспертных оценок, которому присущ ряд ограничений, в том числе: субъективность; отсутствие полноты; сложная повторяемость процесса, как показывает практика ИБ, не обеспечивает формирования исчерпывающего перечня мер по ЗИ, поскольку на практике реализовать непрерывную экспертную оценку рисков ИБ оказывается невозможным.

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 компьютерных атак и идентификации ее параметров, основанная на положениях теории положений криминологии;

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

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

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 характеристик 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 при Минобрнауки России и Аттестационным советом УрФУ, включая 2 в изданиях, индексируемых в международных цитатно-аналитических базах.

Практическая значимость результатов диссертации

Практическая значимость результатов диссертации заключается в обоснованном выборе набора источников информации, обеспечивающих идентификацию параметров разработанных моделей; подтверждении адекватности методики прогнозирования динамики векторов КА с позиции нарушителя, позволяющей 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)и включает в себя введение, три главы, заключение, список сокращений, список литературы из 178 наименований, 8 приложений.

Первая глава посвящена анализу предметной области, в том числе анализу нормативно-правовой базы Российской Федерации, регламентирующей подходы к оценке угроз КА, международных стандартов по оценке угроз и рисков ИБ, проведен анализ

основных научных подходов в области оценки угроз ИБ. Сформулированы ограничения существующих подходов, свидетельствующие о необходимости разработки новой методики прогнозирования вектора динамики КА. На основании результатов анализа состояния предметной области сформулированы цель и задачи исследования.

Вторая глава посвящена обоснованию 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, подходы к выявлению уязвимостей, теория положений криминологии, в которой учитывается экономическая мотивация совершаемого преступления и теория диффузии инноваций.

Третья глава посвящена разработке методики прогнозирования динамики вероятности проведения КА, основанной на использовании предложенных математических моделях, и подтверждению ее работоспособности.

Проведен анализ общедоступных источников информации о КА (более 30), в частности, статистические данные производителей средств ЗИ, которые зачастую не могут быть использованы из-за отсутствия в них абсолютных значений; данные из DarkNet; отчеты центров мониторинга инцидентов ИБ; новостные агрегаторы.

Разработана методика прогнозирования вектора КА. Также автором проведена апробация методики прогнозирования вектора целевых и нецелевых КА, с использованием полученной информации о более чем 700 тысячах обнаруженных КА (анализа КА, реализуемых через заражение популярных сайтов; анализа КА, реализуемых с использованием вредоносного программного обеспечения или социальной инженерии на организации кредитно-финансового сектора).

Замечания и вопросы по работе

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

1. В диссертационной работе при разработке математической модели, описывающей динамику возможности реализации компьютерной атаки во времени не представлено результирующее аналитическое выражение, учитывающее характеристики развития компьютерных атак во времени.

2. Предложенная в работе методика прогнозирования динамики вероятности проведения компьютерных атак во времени с позиции нарушителя не в полной мере

учитывает многообразие возможных вариантов реализации целевых компьютерных атак нарушителей с высоким потенциалом.

3. При оценке ожидаемой полезности компьютерной атаки для нарушителя не в полной мере учитываются факторы, влияющие на развитие компьютерной атаки с учетом существующего множества вариантов и целей реализации компьютерных атак. Для отдельных видов атак понятие полезности следует уточнить, так как выгода нарушителя не всегда оценивается экономическими показателями.

Сделанные замечания имеют дискуссионный характер и 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
Сотрудник Академии ФСО России
Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
Тел.: +7 (4862) 54-99-16
e-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: 302015, г. Орел, ул. Приборостроительная, 35

Козачок Александр Васильевич

26 ноября 2021 г.

Подпись сотрудника Академии ФСО России доктора технических наук, доцента Козачка Александра Васильевича заверяю.

Начальник кадрового аппарата Академии ФСО России

А.Б. Семибратов