ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук Зыряновой Татьяны Юрьевны 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

Методология оценки угроз безопасности информации (БИ) базируется на «Методике оценки угроз безопасности информации», разработанной ФСТЭК России, оценка угроз ИБ осуществляется с помощью метода экспертных оценок. При этом в методических документах ФСТЭК России обозначены риски использования экспертного метода. А именно, независимо от результата формирования экспертной группы при оценке угроз БИ существуют субъективные факторы, связанные с психологией принятия решений. Возможные риски:

- занижение или завышение экспертами прогнозов при оценке угроз БИ;
- пропуск отдельных угроз БИ;
- выделение неоправданных затрат на нейтрализацию неактуальных угроз.

При этом, априори, понятно, что привлечение на практике группы независимых экспертов информационной безопасности (ИБ) с одинаково высоким уровнем компетенции весьма проблематично.

В настоящее время отечественными и зарубежными специалистами в области обеспечения ИБ проводятся активные исследования с целью определения и прогнозирования возможных векторов компьютерной атаки (КА), что подтверждает актуальность темы исследования, указанную в работе.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научные результаты:

научно обоснована математическая модель оценки вероятности реализации нарушителем 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 программно-аппаратного комплекса «Ampire» (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.

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 точки зрения 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). Она состоит из введения, трех глав, заключения, списка сокращений, списка литературы из 178 наименований, 8 приложений.

В первой части работы представлен анализ российских и международных методологий оценки угроз и рисков ИБ, а также подходов к формированию мер защиты информации, основных научных подходов в области оценки угроз ИБ. Сформулированы ограничения существующих подходов, свидетельствующие о необходимости разработки новой методики прогнозирования динамики вектора КА. На основании результатов анализа состояния предметной области сформулированы цель и задачи исследования.

Во второй части работы проведена научно обоснованная разработка математической модели оценки вероятности реализации нарушителем КА и идентификации ее параметров, основанная на положениях ТПК, а также подтверждена ее адекватность результатами как натурного моделирования КА с помощью ПАК «Ampire», так и путем анализа КА, реализованной с помощью вредоносного программного обеспечения (ВПО) Petya.

Кроме того, научно обоснованы принципы и подходы к построению и разработке математической модели, описывающей динамику распространения КА на основе ТДИ, описанной в работах Э. Роджерса, Ф. Басса, Э. Мэнсфилда и Т. Хагерстранда. Практическое подтверждение математической модели проведено путем: анализа динамики КА, реализованной с помощью ВПО WannaCry; натурного моделирования КА с помощью ПАК «Ampire»; прогнозирования целевых и нецелевых КА (спам-атак; КА, реализуемых через заражение популярных сайтов; КА, реализуемых с использованием ВПО или социальной инженерии) на организации кредитно-финансовой сферы.

В третьей части работы представлена разработанная методика прогнозирования вектора КА на базе статистических данных, детально описаны этапы реализации методики и источники получения исходных данных.

Кроме того, в третьей части, после анализа возможных источников информации о КА, сделаны обоснованные выводы, что в качестве источника исходных данных при прогнозировании вероятности КА целесообразно использовать данные из DarkNet, отчеты центров мониторинга инцидентов ИБ, а также информацию, предоставляемую новостными агрегаторами и доступную бухгалтерскую отчетность.

Представлено практическое применение методики при прогнозировании вектора целевых и нецелевых КА, полученное на основе использования информации о более чем 700 тысячах обнаруженных КА (анализа КА, реализуемых через заражение популярных сайтов; анализа КА, реализуемых с использованием ВПО или социальной инженерии) на организации кредитно-финансового сектора.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по содержанию диссертационной работы.

1. В качестве исходных данных оценки возможной полезности от КА для нарушителя рассматривается соотношение возможной материальной выгоды от успешной реализации КА и возможных потерь в случае обнаружения КА. Однако общеизвестны и другие виды мотивации нарушителей, отличные от получения материальной выгоды, такие как: дестабилизация деятельности целевых организаций, получение конкурентных преимуществ, желание самореализации, месть. Очевидно, что в финансовом выражении оценить выгоду, получаемую нарушителем от реализации КА, обусловленных подобной мотивацией невозможно. Рассматривались ли автором перспективы развития предложенной методики на случай прогнозирования действий нарушителей, обусловленных целью получения нематериального результата?
2. В разделе 3.2 диссертационной работы сказано, что предложенную методологию можно использовать для различных известных типов нарушителей, таких как специальные службы иностранных государств, отдельные физические лица (хакеры), конкурирующие организации. Приведен обоснованный вывод о том, что динамика развития КА зависит не от типа нарушителя, а от знаний и возможностей получать знания о методах проведения КА. Есть ли необходимость учитывать в модели другие ресурсы осуществления КА, такие как, например, техническая оснащенность нарушителя или время, имеющееся у нарушителя для осуществления доступа к атакуемым ресурсам?
3. В разделе 3.4 диссертационной работы приведен прогноз тренда КА на 2019 год на основании данных за 2017 и 2018 годы, который оказался не противоречащим фактическим данным за 2019 год, что в полной мере подтверждает адекватность построенной модели и работоспособность предложенной методики

прогнозирования векторов КА. Но данный прогноз составлялся на основании анализа параметров функционирования целевых организаций в штатном режиме. Возможно ли в предложенной модели учесть воздействие дестабилизирующих факторов, имеющих слабопрогнозируемый или даже случайный характер? Например, таких как «локдаун» 2020 года и вынужденный перевод большинства функций целевых организаций в дистанционный режим работы

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 паспорту 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:

Кандидат технических наук
Доцент кафедры «Информационные технологии и защита информации»
Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения»
Тел.: +7 (912) 24-36-956
e-mail: tzyryanova@usurt.ru
Адрес: 620034, г. Екатеринбург, ул. Колмогорова, д.66.

02.12.21

Зырянова Татьяна Юрьевна

Подпись Зыряновой Татьяны Юрьевны заверяю.

Специалист по кадрам А. И. Юрлова