ВВЕДЕНИЕ

Защита информации (ЗИ) предусмотрена Статьей 16 Федерального закона (ФЗ) от 27.07.2006 «Об информации, информационных технологиях и о защите информации» [1], а также иными нормативно-правовыми актами, разработанными государственными регуляторами в области информационной безопасности (ИБ). Данные документы предусматривают применение типовых наборов методов и средств ЗИ, сформированных на базе типовых моделей угроз ИБ, созданных ФСТЭК России и ФСБ России [2–4]. При этом действующим законодательством предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми моделями угроз (МУ) [5–7]. В соответствии с «Методикой оценки угроз БИ», разработанной ФСТЭК России [5], оценка угроз ИБ осуществляется с помощью метода экспертных оценок.

Международные стандарты [8–16] для оценки угроз ИБ предлагают использовать:

- методологию *IT-Grundschutz*, которая в одних случаях рекомендует использовать в организациях и информационных системах (ИС) набор мер ЗИ, состав которого определен на основе сценариев негативных последствий для активов организации, в других — также использовать дополнительный перечень мер ЗИ, формируемых экспертным путем;
- методологию ISO 2700x, рекомендующую формировать набор требований по ЗИ на основе оценки рисков ИБ, которая осуществляется экспертным путем в соответствии с внутренним положением организации по оценке рисков ИБ (при этом ответственность за принятие рисков в целом несет руководитель организации (владелец активов)).

Необходимо отметить, что метод экспертных оценок, которому, как показывает практика ИБ, присущ ряд ограничений (в том числе субъективность, отсутствие полноты или избыточность, сложная повторяемость процесса) не обеспечивает формирования исчерпывающего перечня мер по ЗИ. При этом, очевидно,

что данный метод предназначен для получения оценок угроз ИБ в конкретный момент времени, но не для их прогнозирования в последующие моменты времени.

В этой связи были предприняты многочисленные попытки модернизации действующих международных стандартов и нормативно-правовых документов в области обеспечения ИБ с целью автоматизации процесса формирования профилей ЗИ, использования соответствующих методов визуализации, повышения эффективности экспертной оценки, а также специальных методов ее проведения [17–30]. Необходимо отметить, что оценки угроз и рисков ИБ в данных работах проводились исключительно с точки зрения организации/владельца актива и не имели практических подтверждений результативности и эффективности.

Также отметим работы [31–34], в которых проведен анализ контента форумов *DarkNet*, в первую очередь информации об инцидентах ИБ, вновь разрабатываемых и/или уже известных и активно обсуждаемых на форумах *DarkNet* методах компьютерных атак (КА) с целью прогнозирования соответствующих векторов КА с учетом частоты их упоминаний, а также эмоциональной окраски обсуждений. Данные работы, с нашей точки зрения, следует рассматривать как первые попытки учета информированности нарушителя о методе проведения КА при оценке угроз ИБ, однако не завершившиеся созданием рекомендаций по оценке целесообразности проведения КА с точки зрения нарушителя. В этой связи использование информации, извлекаемой из форумов *DarkNet* для прогнозирования векторов КА, осталась низкой.

Эффективность прогнозов новых уязвимостей программного обеспечения (ПО) с помощью методов одинарного, двойного и тройного экспоненциального сглаживания [35–37], статистических методов (Кростона, ARIMA) [34, 35, 38, 39], кластерного анализа [40, 41], нейронных сетей [35, 42] и машинного обучения [35, 42, 43], основанные на анализе накопленной информации о количестве уязвимостей и их типах в предыдущих версиях, а также и векторов КА, основанных на анализе частоты упоминаний методов КА за определенные временные периоды в *DarkNet* [34], оказались не эффективными, так как существенно расходятся с реальными данными.

При этом необходимо отметить, что данные методы позволяют получать оценки уязвимостей исключительно с точки зрения атакующей стороны. В то же время в экономической и финан-

совых сферах, а также в области предупреждений преступлений общей практики накоплен положительный опыт применения для анализа экономических мотивов преступников «Теории положений о криминологии» (ТПК) Ч. Беккариа и И. Бентама [44–46], которая, однако, при оценке вероятностей КА ранее не использовалась. В этой связи научно обоснованная разработка подходов для оценки угроз ИБ с учетом экономических интересов нарушителя является актуальной.

Целью данной работы является разработка научно обоснованной методики оценивания проведения успешных КА с точки зрения нарушителя вероятностей и прогнозирования динамики их изменения во времени.

Для достижения поставленной цели были сформулированы и решены следующие задачи.

1. Анализ нормативно-правовой базы, регламентирующей подходы к оценке угроз ИБ, и научных подходов, используемых для определения и прогнозирования вектора КА.

2. Разработка и обоснование базовых принципов и подходов к построению математической модели оценки вероятности реализации нарушителем КА и математической модели, описывающей динамику изменения вектора КА во времени, построенного с точки зрения нарушителя.

3. Разработка методики прогнозирования динамики изменения вектора КА, основанной на использовании предложенных математических моделях, и подтверждение ее работоспособности.

Объект исследования: математические модели анализа и прогнозирования КА.

Предмет исследования: методы оценивания с точки зрения нарушителя вероятностей проведения успешных КА, математические модели, описывающие динамику КА, обеспечивающие прогнозирование векторов вероятных КА.

Научная новизна работы заключается в разработке:

1) научно обоснованной математической модели оценки вероятности реализации нарушителем КА и идентификации ее параметров, основанной на положениях ТПК;

2) научно обоснованной математической модели, описывающей динамику возможности реализации нарушителем КА во времени, и идентификация ее параметров, основанной на положениях Теории диффузии инноваций (ТДИ);

3) научно обоснованной методики прогнозирования динамики векторов КА, построенной с точки зрения нарушителя КА.

Теоретическая значимость работы заключается:

1) в обосновании целесообразности применения ТПК, развитой в работах Ч. Беккариа и И. Бентама, для разработки математической модели принятия решения нарушителем о проведении КА;

2) обосновании целесообразности использования ТДИ, развитой в работах Э. Роджерса, Ф. Басса, Э. Мэнсфилда и Т. Хагерстранда, для построения математической модели, описывающей динамику изменения вектора КА во времени.

Практическая значимость работы заключается:

1) в обоснованном выборе набора источников информации, обеспечивающих идентификацию параметров разработанных моделей;

2) подтверждении адекватности методики прогнозирования динамики векторов КА с точки зрения нарушителя, позволяющей выявлять тренды развития КА.

Методология и методы исследований. В работе использованы математическое моделирование, методы системного анализа, ТПК, ТДИ.