УДК 347.775.03 Вестник УрФО № 1(43) / 2022, с. 64–73

Макарова О.С., Поршнев С.В.

DOI: 10.14529/secur220108

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ДИНАМИКИ ВЕРОЯТНОСТИ ПРОВЕДЕНИЯ КОМПЬЮТЕРНОЙ АТАКИ С ТОЧКИ ЗРЕНИЯ НАРУШИТЕЛЯ[1]

В статье отмечается, что методика оценки рисков информационной безопасности (ИБ) имеет ряд существенных ограничений, в частности, используется метод экспертных оценок. Как показывает практика ИБ, метод экспертных оценок имеет ряд ограничений, что в результате не позволяет сформировать необходимый и достаточный перечень мер по защите информации.

В статье детально описаны математические подходы, лежащие в основе методики прогнозирования динамики вероятности проведения компьютерной атаки (КА) с точки зрения нарушителя на основе статистических данных, в частности Теория положений криминологии, и Теория диффузии инноваций.

Отдельно отмечается важность формирования модели нарушителя для определения источников общедоступной информации для расчета вероятности КА. Приведено детальное описание методики прогнозирования динамики вероятности проведения КА с точки зрения нарушителя на основе статистических данных. А также оценка ее адекватности на основе данных о более чем 700 тысячах КА на кредитно-финансовый сектор (КФС) за 2017-2018 гг.

Ключевые слова: *компьютерная атака, прогнозирование вероятности угрозы, модель нарушителя, ожидаемая полезность, нарушитель.*

Makarova O.S., Porshnev S.V.

PREDICTING METHODOLOGY OF THE PROBABILITY DYNAMICS OF A COMPUTER ATTACK FROM THE POINT OF VIEW OF THE INTRUDER

The article notes that the methodology for assessing information security (IS) risks has a number of significant limitations, in particular, the method of expert assessments is used. As the practice of IS shows, the method of expert assessments has a number of limitations, which as a result makes it impossible to form a necessary and sufficient list of measures to protect information.

The article describes in detail the mathematical approaches underlying the methodology for predicting the dynamics of the probability of a computer attack from the intruder point of view based on statistical data, in particular, the Theory of the provisions of criminology, and the Theory of diffusion of innovations.

Separately, the importance of forming a model of the intruder for determining the sources of publicly available information for calculating the probability of an accident is noted. A detailed description of the methodology for predicting the dynamics of the probability of conducting a spacecraft from the point of view of the violator based on statistical data is given. As well as an assessment of its adequacy based on data on more than 700 thousand loans to the credit and financial sector for 2017-2018.

Keywords: *computer attack, threat probability prediction, intruder model, expected utility, intruder.*

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ).

Введение

В действующем законодательстве предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми моделями угроз (МУ) [1-2]. В соответствие с «Методикой оценки угроз БИ», разработанной ФСТЭК России [1], оценка угроз ИБ осуществляется с помощью метода экспертных оценок.

Как показывает практика ИБ, метод экспертных оценок имеет ряд ограничений (в том числе: субъективность; отсутствие полноты или избыточность; сложная повторяемость процесса), что в результате непозволяет сформировать необходимый и достаточный перечень мер по защите информации.

Анализ результатов научных исследований, проведенный в работах [3-10], показал, что в большинстве исследований оценка эффективности и практической применимости предлагаемых подходов и методов оценки угроз БИ и рисков ИБ не проводится. Практические примеры реализации, приводимые в работах [11-15], зачастую используют либо несвязанные с реальными данными значения переменных показателей, либо их экспертные оценки. В этой связи в данной статье описываются математические подходы к определению методики прогнозирования вероятности угроз ИБ с точки зрения нарушителя, алгоритм реализации методики, а также оценка адекватности данной методики.

Математические подходы к описанию методики прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя

Данная методика основана на установленной в работах [4, 5, 8, 9] особенности реализации КА, проявляющейся в том, что вероятность проведения КА нарушителем является условной вероятностью достаточности ожидаемой полезности КА при наличии возможности реализации КА, которая вычисляется по следующей формуле:

$$P(EUA) = P(EU|A)\,P(A), \qquad (1.1)$$

где

P(EUA) – вероятность достаточности ожидаемой полезности КА вида «А» с точки зрения нарушителя;

P(A) – вероятность наличия возможности реализации нарушителем КА вида «А»;

P (EU|A) – условная вероятность ожидаемой полезности КА вида «А» с точки зрения нарушителя, при оценивании которой учитывается возможность незаметного проведения КА.

При этом.

1. Оценки векторов возможных КА, для которых вычисляется оценка вероятности КА на организацию, могут быть получены на основе анализа данных DarkNet, так как нарушители предпочитают использовать известные методы КА, либо адаптировать и дорабатывать их под новую инфраструктуру, чем разрабатывать новые векторы КА.

2. Возможность реализации метода КА и вектора КА, установлена в работе [4, 5, 8, 9], можно оценить в соответствие по следующим формулам

$$Y(t) = \frac{1}{1 + \alpha e^{-\beta t}}, \qquad (1.2)$$

где α, β – параметры модели, называемых s-образными кривыми Перла-Рида.

Согласно исследованиям, проведенным [16] инновация может также развиваться по каскадной модели, описываемой следующей формулой:

$$Y(t) = \begin{cases} \frac{1}{1+\alpha_1 e^{-\beta_1 (t-t_0)}}, \text{ если } t_0 \le t \le t_1, \\ \frac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \frac{1}{1+\alpha_2 e^{-\beta_2 (t-t_1)}}, \text{ если } t_1 < t \le t_2, \\ \cdots \\ \frac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \frac{1}{1+\alpha_2 e^{-\beta_2 (t_2-t_1)}} + \cdots + \frac{1}{1+\alpha_n e^{-\beta_n (t-t_{n-1})}}, \text{ если } t_{n-1} < t \le t_n, \end{cases} \qquad (1.3)$$

где

$[t_0, t_1]$ – длительность первого этапа развития инновации;

$]t_1, t_2]$ – длительность второго этапа развития инновации;

…

$]t_{n-1}, t_n]$ – длительность n-го этапа развития инновации.

3. Оценку достаточности ожидаемой полезности КА можно вычислить по следующей формуле, детальное обоснование такой возможности приведено в [4, 5, 8, 9]:

$$EU = (1 - \rho_n) U(W_m + W_j) + \rho_n U(W_m + W_j - F), \qquad (1.4)$$

где $U(\xi)$ – функция полезности, определенная ниже;

P_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной КА $p_m = 1 - p_n$);

W_m – выгода (прибль) нарушителя в случае успешной реализации КА, с учетом затрат на реализацию КА, определяемая по формуле $W_m = W_{mpj} - C_j$;

C_j – стоимость использованного метода КА;

W_{mpj} – выручка нарушителя в случае успешной реализации КА;

W_j – текущий доход нарушителя от легальной деятельности;

F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте).

4. Оценку вероятности достаточности ожидаемой полезности КА с точки зрения нарушителя, в которой учитывается возможность проведения незаметной КА, можно рассчитывать по формуле (1.1). При этом для нахождения оценок значений параметров функций (1.4), (1.2), (1.3) достаточно использовать информацию из общедоступных источников.

Модель нарушителя, используемая в методике, и ее влияние на компьютерную атаку

В соответствии с нормативными документами ФСТЭК России [1, 2] при формировании модели угроз необходимо разрабатывать модель нарушителя.

Следуя [1], будем использовать следующую классификацию нарушителей, осуществляющих КА в сети Интернет:

– специальные службы иностранных государств;

– отдельные физические лица («хакеры»);

– конкурирующие организации.

Так как порядок этапов проведения КА не зависит от типа нарушителя, то можно использовать предложенную методологию для всех типов нарушителей, при необходимости, корректируя источники общедоступной информации.

Для подтверждения, данного утверждения, рассмотрим два крайних случая:

– нарушителя, не обладающего знаниями в области ИТ и ИБ (например, школьника или пенсионера);

– нарушителя, обладающего неограниченными ресурсами и возможностями получать знания (например, сотрудника специальной службы иностранного государства).

Нарушитель, не обладающий знаниями в области ИТ и ИБ

К данному типу нарушителей можно отнести, например, школьников и студентов младших курсов. Отличительной особенностью данного типа является не знание законодательства РФ, а также отсутствие легального текущего дохода. Поэтому в (1.4), (1.2) достаточно подставить следующие значения $F_j = 0$, $W_j = 0$.

Кроме того, в случае данного типа нарушителя источник с данными об КА можно заменить с данных с форумов DarkNet на данные из Интернета, например Youtube.

Нарушитель, обладающий неограниченным ресурсам и возможностями получать знания

К данному типу нарушителей следует отнести специальные службы иностранных государств. При определении ожидаемой полезности необходимо учитывать, что величина тяжести наказания F_j зависит не от Уголовного кодекса РФ, но от тяжести последствий для иностранного государства при выявлении его причастности к подобной деятельности. В связи с этим, можно сделать вывод, что для сокрытия своего типа нарушитель будет стараться использовать данные, как и любой другой нарушитель, т.е. методы DarkNet.

Это подтверждает и статистика по оценкам [17], количество совершенно нового ВПО, появившегося в период с 3 квартала 2016 г. по 2 квартал 2018 г., составило менее 10% от общего числа ВПО. Так как для реализации КА используется несколько методов КА, то в части этапов реализации КА данным типом нарушителя будут использоваться методы из общедоступных источников информации. Подтверждением данному высказыванию служит то, что многие специалисты считают КА ВПО Petya, реализованной специальными службами.

Таким образом, при прогнозировании вектора КА необходимо определить модель нарушителя, на основании которой необходимо выбирать наиболее подходящие общедоступные источники информации. Сама методология оценивания вероятностей КА при этом не изменится.

Методика прогнозирования динамики вероятности проведения компьютерной атаки с точки зрения нарушителя

Прогнозирование динамики развития КА реализуется на этапе теоретической и практической подготовки с точки зрения нарушителя. Расчет вероятности $P(EUA) = P(EU|A)\,P(A)$ реализуется выполнением последовательности действий, представленную на рис. 1.

Пример практического использования методики прогнозирования динамики компьютерной атаки

Проведем прогнозирование тренда КА в КФС на 2019 г., перечень КА для анализа представлен ниже:

– целевые КА на организации КФС;

– нецелевые (спам-атаки) на организации КФС;

– нецелевые КА на клиентов КФС через зараженные популярные сайты;

– нецелевые КА на клиентов КФС с использованием ВПО;

– нецелевые КА на клиентов с использованием социальной инженерии.

Для это будем использовать статистику Центрального банка за 2017, 2018, 2019 годы [17-20], а также данные новостных агрегаторов о КФС [21].

В качестве нарушителя рассмотрим нарушителя, имеющего доступ в DarkNet, но при этом не обладающего неограниченным ресурсом. Для оценки известности метода КА будем использовать статистику DarkNet [4, 5, 8, 9], для оценки заработной платы – легальной выгоды, воспользуемся данными с сайта Superjob [22].

Используя представленную выше методику получаем значения возможности реализации КА в КФС за 2017 и 2018 год в таблицах 1 и 2, соответственно.

Из таблицы 1 видно, что рентабельность целевых КА на КФС может быть оценена как $1/\alpha_j$, и отрицательна. Таким образом, реализация целевых КА на КФС в том виде, что они были в 2017 году в последующие годы не возможна $p(A) – 0$. Расчеты также показывают, что наиболее активно развиваются КА с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА.

Из таблицы 2 видно, что действительно тип целевых КА на КФС существенно изменился: средняя сумма выручки нарушителя сократилась в 12 раз, так как

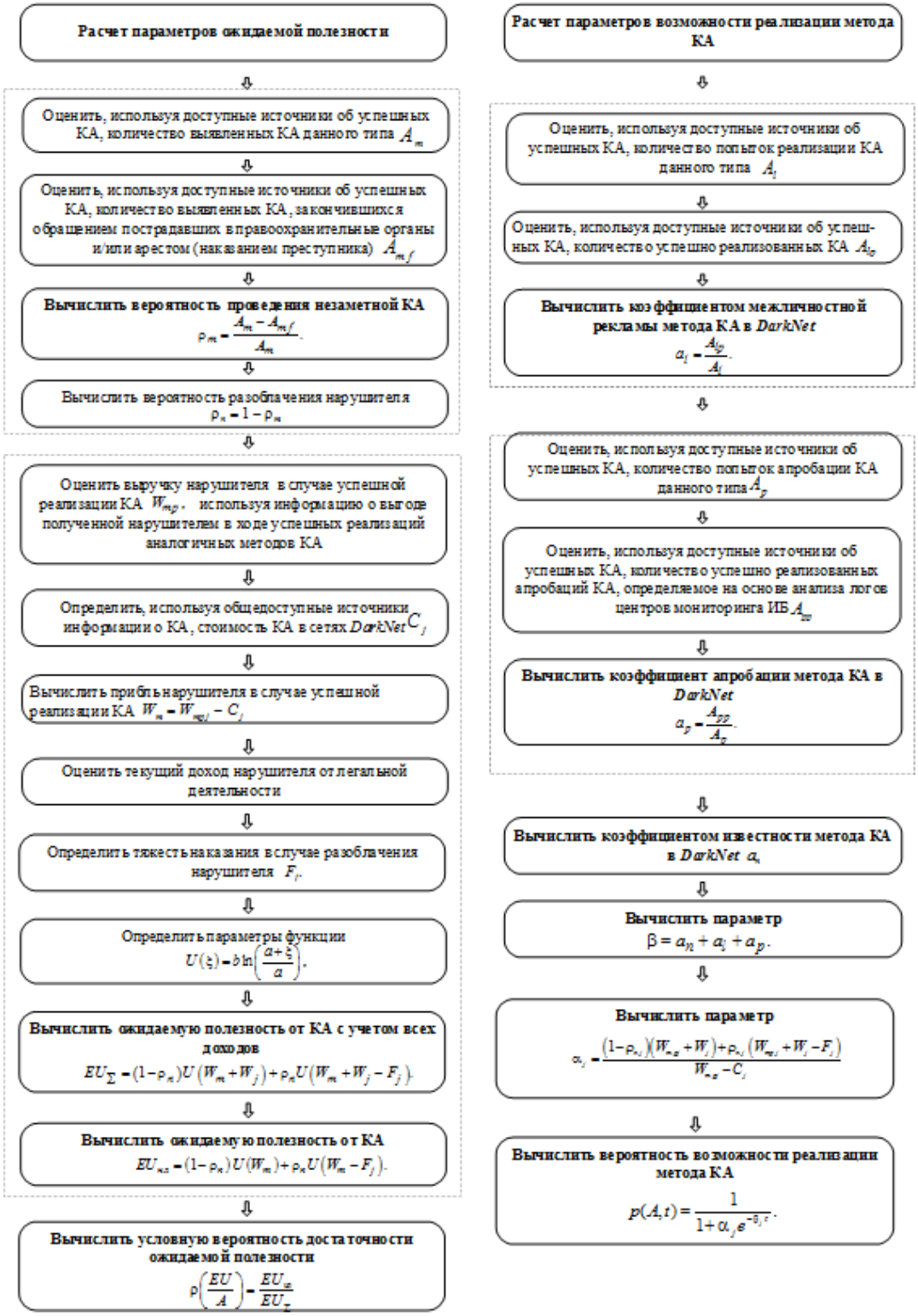

Рис. 1. Методика прогнозирования вектора КА

возросло число попыток замаскировать целевую КА. Однако, видоизменение целевой КА не помогло, так как число уголовных дел в отношении нарушителей, реализовывающих целевые КА на КФС, увеличилось. Логично предположить, что целевые КА на КФС продолжат видоизменяться. В том, числе путем изменения фокуса с КФС на клиентов КФС, о чем свидетельствует увеличение вероятности возможности реали-

Таблица 1

Возможность реализации КА в КФС за 2017 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,278	122,872	0,28	0,949	37	39
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,000	112	0,12	1	200000	200000
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,494	1,023	140	0,4	1	481	481
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,499	1,001	112	0,12	1	63582	63582
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	0,999	129,996	0,3	0,999	27566	27567

Таблица 2

Возможность реализации КА в КФС за 2018 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,941833681	122,44	0,28	0,949	68	72
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,00	112	0,12	1	300000	300000
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,498	1,01	140	0,4	1	2205	2205
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,500	0,999	111,99	0,12	1	1029436	1029438
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	1,00	130	0,3	0,999	36000	36000

зации нецелевых КА на клиентов КФС с использованием ВПО.

Возможность реализации КА с использованием социальной инженерии стабильно высока, что говорит, об активном распространении метода КА среди нарушителей. Это объясняется тем, что одни и те же методы социальной инженерии можно неоднократно применять, так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизованно поменять конфигурацию).

Анализ прогноза на 2019 год

Вероятность ожидаемой полезности при условии возможности реализации КА в 2017 и 2018 гг., а также прогнозное значение вероятности ожидаемой полезности при условии возможности реализации КА за 2019 г. представлены в таблице 3.

Данные, представленные в таблице 3, позволили дать следующий прогноз трендов КА на 2019 г.

1. Целевые КА на организации КФС в том виде, в котором они реализовывались в 2017 и 2018 гг. в 2019 г. реализовываться не будут, так как вероятность ожидаемой полезности при наличии возможности реализации КА данного вида равна нулю. Это означает, что группы злоумышленников будут видоизменять целевые КА (выгода с реализации КА, метод и т.п.), либо будут переходить на нецелевые КА.

2. Увеличится вероятность реализации нецелевых КА на клиентов КФС Об этом свидетельствует смеще-

Таблица 3

Вероятность ожидаемой полезности за 2017, 2018, 2019 гг.

j	Наименование КА	P(EUA) в 2017 г.	P(EUA) в 2018 г.	P(EUA) в 2019 г.
1	Целевые КА на организации КФС	0	0	0
2	Нецелевые (спам-атаки) на организации КФС	0,120	0,121	0,122
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,071	0,078	0,085
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,106	0,121	0,136
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,092	0,107	0,122

ние фокуса внимания нарушителей с КФС на иные сферы бизнеса, так как КФС сумел построить единую централизованную систему оповещения о новых методах КА и оперативного предупреждения инцидентов ИБ, в том числе блокировки КА на уровне операторов связи. В сфере КФС сформировалась практика обращения в правоохранительные органы и доведения дел до суда, чего не скажешь про иные сферы бизнеса.

3. Минимальное значение вероятности нецелевых КА со сравнению с другими КА из таблицы 3 на клиентов КФС через зараженные популярные сайты по сравнению с другими нецелевыми КА. Это объясняется наличием механизма блокировки КА на уровне операторов связи.

4. Увеличится вероятность реализации нецелевых атак на клиентов КФС с использованием ВПО. Увеличение вероятность КА данного типа может быть связано, с тем, что данные КА технологически похожи на целевые КА, при этом они с точки зрения нарушителя не обладают ограничениями целевых КА.

5. Увеличится вероятность реализации нецелевых атак на клиентов с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА. Одни и те же методы социальной инженерии можно неоднократно применять (рентабельность КА возрастает), так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизовано поменять конфигурацию).

В связи с тем, что в отчете Банка России [20, 21] не представлены количественные значения показателей КА за 2019 г., но только качественные описания фактических векторов КА, проведем сравнение спрогнозированной в динамики изменений вероятности КА с аналогичными данными, представленными в отчете.

Выводы

Результаты сравнения показывают, что прогноз динамики изменения векторов КА оказался верным по:

– целевым КА на организации КФС;

– нецелевым (спам-атаки) КА на организации КФС;

– нецелевым КА на клиентов КФС через зараженные популярные сайты;

– нецелевым КА на клиентов КФС с использованием ВПО;

– нецелевым атакам на клиентов с использованием социальной инженерии.

В 2019 г. по данным отчета Банка России:

1. Наблюдалось снижение количества попыток КА на организации КФС. Произошло смещение фокуса внимания злоумышленников с организаций кредитно-финансового сектора на их клиентов. В частности, сохранялась высокая интенсивность распространения нарушителями ВПО класса ransomware (целевых КА), но уже не на КФС.

2. Одним из основных инструментов компьютерных преступников, по-прежнему, оставалось ВПО.

3. В 2019 г. в арсенале злоумышленников появился новый способ обмана жертв -У Банка России появились полномочия по инициированию снятия с делегирования мошеннических интернет ресурсов и построен процесс взаимодействия со всеми участниками процесса разделегирования. (Минимальное время разделегирования доменов фишинговых ресурсов составило 3 часа 3 дня, что стало возможным благодаря появлению дежурной службы, работающий в режиме 24/7/365.)

5. Был осуществлен переход 66% мошеннических ресурсов в юриспруденцию иностранных доменных зон. Что говорит об изменении тренда с нецелевых атак на клиентов КФС через зараженные популярные российские сайты, на западные сайты. (Отметим, что у Банка России нет компетенций на разделегирования фишинговых ресурсов за пределами доменных зон .ru, .рф, .su).

Таким образом, прогноз динамики КА в 2019 г. оказался не противоречащим соответствующим данным Банка России, что подтверждает работоспособность предложенной методики прогнозирования вектора КА.

Выводы

1. Предложена методика прогнозирования векторов КА, позволяющая выявлять тренды развития КА с точки зрения нарушителя.

2. Проведена оценка результатов практической апробации, которая подтвердила, что вектор КА определяется:

2.1. Вероятностью разоблачения нарушителя (вероятность проведения незаметной КА) и тяжестью наказания, для нарушителя. Осуществление защиты от КА возможно за счет изменения восприятия преступником возможностей (в том числе, соотношения между выгодой и потерями) совершения преступления путем повышения возможности разоблачения нарушителя.

2.2. Характеристиками самой КА, в частности, экономичностью и рентабельностью 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).

2.3. На текущий момент доходы от легальной деятельности существенно ниже выручки нарушителя от реализации КА.

Литература

1. Методический документ: Методика оценки угроз безопасности информации: [утвержден ФСТЭК России 5 февраля 2021 г.]. – Доступ из справочно-правовой системы Гарант. – Текст: электронный.

2. Банк данных угроз БИ ФСТЭК России: [сайт]. – URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2019). – Текст: электронный.

3. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2021. — Т. 28. № 2. — С. 6-20.

4. Computer attack`s probability function / Makarova O., Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568.

5. Оценивание вероятностей компьютерных атак на основе функций / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 2. — С. 86-96.

6. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information / Makarova Olga; Porshnev Sergey // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2020. — No. 9117676 — pp. 593-596.

7. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 1. — С. 6-18.

8. Determining the Choice of Attack Methods Approach / Makarova Olga // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. — 2021. — No. 9455072 — pp. 399-402.

9. Mathematical Model of the Computer Attack Implementation Possibility by an Intruder / Makarova Olga; Porshnev Sergey // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455045 — pp. 395-398.

10. Simulation of Computer Attack Scenarios for Industrial Robots from the Point of Intruder View / O. Makarova and M. Lihota // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455052 — pp. 474-477.

11. Белокурова, Е. В. Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем / Е. В. Белокурова, А. А. Дерканосова, А. А. Змеев [и др.]. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2015. – 6 с. – URL: https://cyberleninka.ru/article/n/sposoby-otsenki-ugroz-bezopasnosti-konfidentsialnoy-informatsii-dlya-informatsionno-telekommunikatsionnyh-sistem/viewer (дата обращения: 08.07.2021).

12. Налини М. Digital risk management for data attacks against state evaluation = Цифровое управление рисками для атак на данные против оценки состояния / М. Налини, А. Чакрам // International Journal of Innovative Technology and Exploring Engineering (IJITEE). – 2020. – № 88. – DOI: https://doi.org/10.35940/ijitee.I1130.0789S419. – Текст: электронный (дата обращения: 08.07.2021).

13. Зикратов И. А. Evaluation of information security in cloud computing based on the bayesian approach = Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода / И. А. Зикратов, С. В. Одегов. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2012. – 6 с. – URL: https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda/viewer (дата обращения: 08.07.2021).

14. Скворцова М. А. Разработка системы поддержки принятия решения для оценки рисков и угроз национальной безопасности / М. А. Скворцова, В. И. Терехов. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2018. – 11 с. – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer (дата обращения: 08.07.2021).

15. Кузнецов Н. А. Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов / Н. А. Кузнецов, А. А. Мозоль. – Текст: электронный // Электронная библиотека: КиберЛенинка: [сайт]. – 2019. – 7 с. – URL: https://cyberleninka.ru/article/n/model-avtomatizirovannoy-sistemy-optimizatsii-parametrov-upravleniya-riskami-v-terminah-ugroz-uyazvimostey-i-rezervov/viewer (дата обращения: 08.07.2021).

16. Хагерстранд Т. Innovation diffusion as a spatial process= Дифуззия инновации как пространственный процесс / Т. Хагерстранд // Chicago, University of Chicago Press. – 1967. – DOI: https://doi.org/10.1111/j.1538-4632.1969.tb00626.x. – Текст: электронный (дата обращения: 08.07.2021).

17. Чои С. A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments = Исследование по анализу информации о поведении вредоносного кода для прогнозирования угроз безопасности в новых средах / С. Чои, Т. Ли, Д. Квак // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – С. 1611–1625. – DOI: https://doi.org/10.3837/tiis.2019.03.028. – Текст: электронный (дата обращения: 08.07.2021).

18. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2017 – 31.08.2018. – Текст. Изображение: электронные // Банк России: [сайт]. – 2018. – URL: http://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf (дата обращения: 27.04.2020).

19. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – Текст. Изображение: электронные // Банк России [сайт]. – 2018. – URL: http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf (дата обращения: 27.04.2020).

20. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2018 – 31.08.2019. – Текст. Изображение: электронные // Банк России: [сайт]. – 2019. – URL: http://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (дата обращения: 17.11.2019).

21. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. – Текст. Изображение: электронные // Банк России: [сайт]. – 2021. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 08.07.2021).

22. Зарплатный индекс Superjob сферы «Информационные технологии». – Текст. Изображение: электронные // SuperJob: [сайт]. – 2017. – URL: https://www.superjob.ru/paymentindex/it/#/31 (дата обращения: 08.07.2021).

23. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем / Макарова О.С., Поршнев С.В. // Безопасность информационных технологий. — 2021. — Т. 28. № 2. — С. 6-20. (1,5 п.л. / 0,75 п.л.)

References

1 Metodicheskiy dokument: Metodika otsenki ugroz bezopasnosti informatsii: [utverzhden FSTEK Rossii 5 fevralya 2021 g.]. – Dostup iz spravochno-pravovoy sistemy Garant. – Tekst: elektronnyy.

2 Bank dannykh ugroz BI FSTEK Rossii: [sayt]. – URL: https://bdu.fstec.ru/ (data obrashcheniya: 17.11.2019). – Tekst: elektronnyy.

3 Opredeleniye parametrov, vliyayushchikh na vozmozhnost' realizatsii komp'yuternoy ataki narushitelem / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2021. — T. 28. № 2. — S. 6-20.

4 Computer attack`s probability function / Makarova O., Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568.

5 Otsenivaniye veroyatnostey komp'yuternykh atak na osnove funktsiy / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2020. — T. 27. № 2. — S. 86-96.

6 Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information / Makarova Olga; Porshnev Sergey // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2020. — No. 9117676 — pp. 593-596.

7 Otsenivaniye veroyatnostey komp'yuternykh atak na osnove metoda analiza iyerarkhiy s dinamicheskimi prioritetami i predpochteniyami / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2020. — T. 27. № 1. — S. 6-18.

8 Determining the Choice of Attack Methods Approach / Makarova Olga // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. — 2021. — No. 9455072 — pp. 399-402.

9 Mathematical Model of the Computer Attack Implementation Possibility by an Intruder / Makarova Olga; Porshnev Sergey // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455045 — pp. 395-398.

10 Simulation of Computer Attack Scenarios for Industrial Robots from the Point of Intruder View / O. Makarova and M. Lihota // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455052 — pp. 474-477.

11 Belokurova, Ye. V. Sposoby otsenki ugroz bezopasnosti konfidentsial'noy informatsii dlya informatsionno-telekommunikatsionnykh sistem / Ye. V. Belokurova, A. A. Derkanosova, A. A. Zmeyev [i dr.]. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2015. – 6 s. – URL: https://cyberleninka.ru/article/n/sposoby-otsenki-ugroz-bezopasnosti-konfidentsialnoy-informatsii-dlya-informatsionno-telekommunikatsionnyh-sistem/viewer (data obrashcheniya: 08.07.2021).

12 Nalini M. Digital risk management for data attacks against state evaluation = Tsifrovoye upravleniye riskami dlya atak na dannyye protiv otsenki sostoyaniya / M. Nalini, A. Chakram // International Journal of Innovative Technology and Exploring Engineering (IJITEE). – 2020. – № 88. – DOI: https://doi.org/10.35940/ijitee.I1130.0789S419. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

13 Zikratov I. A. Evaluation of information security in cloud computing based on the bayesian approach = Otsenka informatsionnoy bezopasnosti v oblachnykh vychisleniyakh na osnove bayyesovskogo podkhoda / I. A. Zikratov, S. V. Odegov. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2012. – 6 s. – URL: https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda/viewer (data obrashcheniya: 08.07.2021).

14 Skvortsova M. A. Razrabotka sistemy podderzhki prinyatiya resheniya dlya otsenki riskov i ugroz natsional'noy bezopasnosti / M. A. Skvortsova, V. I. Terekhov. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2018. – 11 s. – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer (data obrashcheniya: 08.07.2021).

15 Kuznetsov N. A. Model' avtomatizirovannoy sistemy optimizatsii parametrov upravleniya riskami v terminakh ugroz, uyazvimostey i rezervov / N. A. Kuznetsov, A. A. Mozol'. – Tekst: elektronnyy // Elektronnaya biblioteka: KiberLeninka: [sayt]. – 2019. – 7 s. – URL: https://cyberleninka.ru/article/n/model-avtomatizirovannoy-sistemy-optimizatsii-parametrov-upravleniya-riskami-v-terminah-ugroz-uyazvimostey-i-rezervov/viewer (data obrashcheniya: 08.07.2021).

16 Khagerstrand T. Innovation diffusion as a spatial process= Difuzziya innovatsii kak prostranstvennyy protsess / T. Khagerstrand // Chicago, University of Chicago Press. – 1967. – DOI: https://doi.org/10.1111/j.1538-4632.1969.tb00626.x. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

17 Choi S. A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments = Issledovaniye po analizu informatsii o povedenii vredonosnogo koda dlya prognozirovaniya ugroz bezopasnosti v novykh sredakh / S. Choi, T. Li, D. Kvak // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – S. 1611–1625. – DOI: https://doi.org/10.3837/tiis.2019.03.028. – Tekst: elektronnyy (data obrashcheniya: 08.07.2021).

18 Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno-finansovoy sfere departamenta informatsionnoy bezopasnosti Banka Rossii 01.09.2017 – 31.08.2018. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2018. – URL: http://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf (data obrashcheniya: 27.04.2020).

19 Obzor osnovnykh tipov komp'yuternykh atak v kreditno-finansovoy sfere v 2018 godu. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii [sayt]. – 2018. – URL: http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf (data obrashcheniya: 27.04.2020).

20 Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno-finansovoy sfere departamenta informatsionnoy bezopasnosti Banka Rossii 01.09.2018 – 31.08.2019. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2019. – URL: http://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (data obrashcheniya: 17.11.2019).

21 Osnovnyye tipy komp'yuternykh atak v kreditno-finansovoy sfere v 2019–2020 godakh. – Tekst. Izobrazheniye: elektronnyye // Bank Rossii: [sayt]. – 2021. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (data obrashcheniya: 08.07.2021).

22 Zarplatnyy indeks Superjob sfery «Informatsionnyye tekhnologii». – Tekst. Izobrazheniye: elektronnyye // SuperJob: [sayt]. – 2017. – URL: https://www.superjob.ru/paymentindex/it/#/31 (data obrashcheniya: 08.07.2021).

23 Opredeleniye parametrov, vliyayushchikh na vozmozhnost' realizatsii komp'yuternoy ataki narushitelem / Makarova O.S., Porshnev S.V. // Bezopasnost' informatsionnykh tekhnologiy. — 2021. — T. 28. № 2. — S. 6-20. (1,5 p.l. / 0,75 p.l.)

МАКАРОВА Ольга Сергеевна, кандидат технических наук, руководитель регионального представительства в Уральском федеральном округе кампании «ИнфоТекс», старший преподаватель Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 2, e-mail: o.s.makarova@urfu.ru

MAKAROVA Olga Sergeevna, Candidate of Technical Sciences, Head of the Regional Representative Office of the InfoTeKS company in the Ural Federal District, Senior Lecturer of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin», 620002, Yekaterinburg, st. Mira, 32, e-mail: o.s.makarova@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. e-mail: s.v.porshnev@urfu.ru