Ольга С. Макарова[1], Сергей В. Поршнев[1,2]
*[1]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, ул. Мира, 19, Екатеринбург, 620002, Россия*
*[2]Институт математики и механики Уральского отделения Российской академии наук, ул. Софьи Ковалевской, 16, Екатеринбург, 620108, Россия*
*[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702*
*[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350*

# ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ С ДИНАМИЧЕСКИМИ ПРИОРИТЕТАМИ И ПРЕДПОЧТЕНИЯМИ

*DOI: http://dx.doi.org/10.26583/bit.2020.1.01*

*Аннотация.* Задача получения адекватных оценок вероятностей угроз и рисков информационной безопасности (ИБ), а также прогнозирования векторов вероятных атак нарушителей, используя новые методы, в связи с активным использованием информационных технологий в различных организациях становится все более актуальной. В статье обоснован новый метод прогнозирования вероятности компьютерных атак, рассматриваемых с позиции приоритетов нарушителя, основанный на использовании метода анализа иерархий с динамическими приоритетами и предпочтениями. Для практического использования данного метода обоснован выбор ключевых факторов атаки, а также проведен сравнительный анализ предложенного и известных методов прогнозирования вероятностей атак, что позволило выявить его преимущества и ограничения. Получены оценки вероятностей компьютерных атак в 2019 г.
*Ключевые слова: прогнозирование, информационная безопасность, кибербезопасность, нарушитель, вероятность угроз, метод функционального выбора, ключевые факторы атаки.*
*Для цитирования: МАКАРОВА, Ольга С.; ПОРШНЕВ, Сергей В. ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ С ДИНАМИЧЕСКИМИ ПРИОРИТЕТАМИ И ПРЕДПОЧТЕНИЯМИ.Безопасность информационных технологий, [S.l.], v. 27, n. 1, p. 6-18, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1248>. Дата доступа: 10 feb. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.*

Olga S. Makarova[1], Sergey V. Porshnev[1,2]
*[1]Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B.N. Yeltsin", 19 Mira Str., Ekaterinburg, 620002, Russia*
*[2]Institute of mathematics and mechanics of the Ural branch of the Russian Academy of Sciences, Sophia Kovalevskaya Str., 16, Ekaterinburg, 620108, Russia*
*[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702*
*[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350*

# Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences

*DOI: http://dx.doi.org/10.26583/bit.2019.4.01*

*Abstract.* The task of obtaining adequate assess of the threat`s probability and risks of information security as well as forecasting the vectors of likely attacks of hackers using new methods has become rather relevant with active penetration of information technologies (IS) in organizations. This study substantiates a new method for predicting the probability of computer attacks considered from the perspective of the offender's priorities. This method is based on analyzing hierarchies with dynamic priorities and preferences. For practical use the choice of key attack factors was justified and a comparative analysis of the proposed and already known methods for predicting the probability of attacks

is carried out. This has helped us to identify its advantages and limitations. Estimates of the probability of computer attacks in 2019 were obtained.
*Keywords: forecasting, information security, cyber security, hacker, threats probability, functional decision making method, key attack criteria.*
*For citation: MAKAROVA, Olga S.; PORSHNEV, Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.], v. 27, n. 1, p. 6-18, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1248>. Date accessed: 10 feb. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.*

## Введение

За последние три года было реализовано несколько крупных публично обнародованных компьютерных атак на крупные государственные корпорации, банки, коммерческие организации и организации малого и среднего бизнеса, которые показали не состоятельность существующих систем защиты компьютерных систем и сетей [1–3]. Анализ причин, которые делают системы ИБ предприятий и организаций несостоятельными, показывает, что их можно разделить на следующие классы:

1) причины, обусловленные действиями внутренних сотрудников;
2) причины, обусловленные внешними компьютерными атаками.

Например, в 2017 г. по данным ведущих отечественных разработчиков средств защиты Positive Technologies, Infowatch и Solar Security 48% от общего числа атак составили причины первого класса, 52% от общего числа атак – причины второго класса. Отметим, что при этом 95% российских компаний, подвергшихся атакам, на момент атаки использовали средства защиты информации, построенные либо на классическом подходе, основанном на требованиях законодательства Российской Федерации, либо на международных практиках, в основе которых лежит оценка рисков, либо на смешенном варианте, объединяющем данные подходы.

Напомним, что классическая методология рекомендует при формировании системы ИБ строить модели нарушителей и модели угроз [4]. При этом в зависимости от класса защищаемых информационных систем (ИС) в законодательстве РФ определены жесткие требования к реализации систем ИБ [5]. Традиционно, система защиты строится:

– с помощью статистической модели угроз, базирующейся на типовом перечне угроз [6];

– с учетом типов нарушителя по уровню доступа к компонентам инфраструктуры организации;

– на базе статической матрицы усредненных требований к системе защиты, имеющей относительно небольшое количество градаций/вариаций (для конкретной организации данные требования могут оказаться избыточными или недостаточными);

– в определенном временном сечении (на дату построения);

– основываясь на информации о защищаемой ИС, зачастую без учета взаимодействия с другими ИС данной организации.

Международный подход [7] отличается от подхода, используемого в законодательстве РФ, отсутствием четко определенных требований к системе ИБ, которые предлагается формировать на базе оценки рисков ИБ и вероятности угроз ИБ. Здесь отсутствуют формализованные требования и четкий перечень возможных угроз. Это обеспечивает формирование гибкой модели угроз, а также точечный, а потому потенциально эффективный, подбор компонентов системы защиты. При этом вероятность реализации угрозы оценивается исходя из возможности нарушения конфиденциальности, целостности и доступности защищаемой информации из-за наличия угроз и уязвимостей в ИС. Отметим, что здесь, как и в классическом подходе, учитывается только тип нарушителя, определяемый уровнем

доступа к компонентам инфраструктуры организации. При этом, однако, оценка вероятности угроз ИБ оказывается краткосрочной, так как не учитываются возможные изменения вектора атаки в течение времени. Кроме того, в обсуждаемых подходах не учитываются следующие ключевые факторы атаки:

1) у нарушителя:
- мотивы нарушителя;
- критерии выбора объекта атаки нарушителем;
- этапы и методы реализации атаки;
- методы получения информации об объекте;
- принципы принятие решения о проведении/продолжении/прекращении атаки нарушителем.

2) изменения во времени:
- типа, характера и навыков нарушителя;
- компонентов, архитектуры и настроек защищаемой ИС;
- компетенций сотрудников, как рядовых, так и привилегированных.

В результате «мгновенные» оценки вероятности угроз ИБ и соответствующих рисков для ИС, оказавшиеся не высокими в данный момент времени, в дальнейшем, поскольку нарушитель, будучи необнаруженным, имеет возможность в течение длительного времени собирать информацию о средствах защиты внешнего и внутреннего периметра ИС и готовить результативную атаку [1–3], могут оказаться не состоятельными. Таким образом, разработка подходов, обеспечивающих получение динамических оценок вероятности угроз ИБ и соответствующих рисков ИБ для ИС, являются актуальным.

В статье обосновывается методика динамического оценивания вероятности угроз ИБ с позиции нарушителя.

## 1. Постановка задачи оценки вероятности использования типов атак

Под угрозой будем понимать совокупность множества источников угрозы, множества способов реализации угрозы, множества используемых уязвимостей и объекта (актив), подвергаемого угрозе [4].

Обозначим множество всех угроз, известных в момент времени $t_1$, как

$$У_1 = \{y_{11}, y_{12}, \dots y_{1i}, \dots y_{1g}\},$$

где $g$ – количество всех угроз в момент времени $t_2$:

$$У_2 = \{y_{21}, y_{22}, \quad y_{2i}, \quad y_{2d}\},$$

где $d \geq g$.

Обозначим вероятность соответствующих угроз:

$$p_{y1} = \{p_{y11}, p_{y12}, \dots p_{y1i}, \dots p_{y1g}\},$$

где $i$ – номер угрозы из множества $У_1$, в момент времени $t_1$,

$$p_{y2} = \{p_{y21}, p_{y22}, \dots P_{y2i}, \dots \quad p_{y2d}\},$$

где $i$ – номер угрозы из множества $У_2$ в момент времени $t_2$.

При оценке угрозы объекта (актива), следуя [4, 7], будем принимать во внимание, что атака – это комплекс действий (способы реализации угрозы) нарушителя (источника угроз), направленных на поиск и эксплуатацию уязвимостей объекта для реализации целей (мотивов нарушителя) на объекте (активе) в определенное время с определенным

бюджетом не приводящий к обнаружению нарушителя. Цель атаки на объект заключается в нарушении конфиденциальности, целостности, доступности информации.

Обозначим множество атак:

$$M_1 = \{m_{11}, m_{12}, \dots m_{1j}, \dots m_{1e}\},$$

где $e$ – количество атак в момент времени $t_1$,

$$M_2 = \{m_{21}, m_{22}, \dots, m_{2j}, \dots, m_{2e}\},$$

где $e$ – количество атак в момент времени $t_2$.

Обозначим множество вероятностей использования атак в момент времени $t_1$:

$$p_{m1} = \{p_{m11}, p_{m12}, \dots, p_{m1i}, \dots, p_{m1e}\},$$

где $p_{m1i}$ – вероятность $i$-ой атаки в момент времени $t_1$,

$$p_{m2} = \{p_{m21}, p_{m22}, \dots p_{m2i}, \dots p_{m2e}\},$$

где $p_{m2i}$ – вероятность $i$-ой атаки в момент времени $t_2$.

В первом приближении будем считать, что на каждом этапе нарушитель может использовать только одну атаку. Возможную атаку будем характеризовать мотивами нарушителя, критериями выбора объекта атаки, этапами атаки, информацией об объекте и принятых решениях о проведении, продолжении или прекращении атаки нарушителем. Таким образом, в качестве показателей для получения оценки вероятности использования типов атак можно использовать:

1) выгоду атакующего в случае успешной реализации атаки (Выгода);
2) незаметность атаки, гарантирующую защиту от преследования и наказания нарушителя;
3) длительность атаки, будем считать, что атака эффективнее при меньшей длительности;
4) доступность (известность) методов для реализации атаки.

С учетом вариантов разделения атаки [8] выделим следующие этапы действий атакующего:

1) Разведка внешнего периметра.
2) Подготовка плацдарма для атаки.
3) Преодоление периметра путем эксплуатации «внешних» уязвимостей.
4) Разведка внутреннего периметра/выбор цели атаки.
5) Подготовка плацдарма для атаки.
6) Реализация атаки.
7) «Зачистка».

Множество атак $M$ в соответствие с выбранными этапами действий атакующего можно разделить на группы атак по этапам:

$$m_\alpha = \{m_{\alpha 1}, m_{\alpha 2}, \dots m_{\alpha j}, \dots m_{\alpha k}\},$$

где α – номер этапа действий нарушителя, $k$ – номер типа атаки, как правило, $k < 10$.

Решаемая задача состоит в прогнозировании на основе анализа информации об атаках и в порядке типов атаки, упорядоченных в соответствии с критериями, определяющими атаку, в моменты времени $t_1$, $t_2$ и вероятности атак в момент времени $t_3$.

## 2. Анализ методов прогнозирования вероятности компьютерных атак

Из описания задачи оценивания вероятности угроз (атак) ИБ, приведенного в предыдущем разделе видно, что по своей постановке она оказывается аналогичной задачам, возникающим при управлении социальными, экономическими, производственными, политическими и иными сложными системами [10, 11, 13].

Для решения данного типа задач, традиционно, используют методы исследования операций, методы критериального выбора (метод Парето-доминирования, лексиминная оптимизация, лексикографическая оптимизация, метод вербального анализа решений) [10], методы функционального выбора (метод оптимизации по достижению цели, метод многокритериальной оптимизации с предварительным отбором, метод упорядочения по образцу, метод оптимизации по индивидуальным целям) [10, 11, 13]. Однако, данные методы требуют предварительного отображения выбранных показателей атаки соответствующие квантитативные шкалы, а также знания функций, описывающих зависимости вероятности атаки от выбранных критериев, нахождение которых является сложной самостоятельной задачей, универсальных методов решения которой в настоящий момент не найдены. Также отметим, что данные методы не гарантируют автоматического упорядочения атак.

В этих условиях представляется целесообразным использовать метод анализа иерархий (МАИ), основанный на представлении исследуемой системы в виде некоторой иерархической структуры, создаваемой на основе метода экспертных оценок, который демонстрирует свою результативность даже при относительно небольшом числе привлеченных экспертов (менее 10). Отметим, что здесь не требуется проводить анализ данных больших размерностей, так как эксперт может адекватно/эффективно проводить умозрительный анализ данных размерностью 7±2 [10].

Напомним, что в МАИ исходные данные формируются путем попарных сравнений альтернатив (атак) по заранее выбранной шкале [13]. В рамках данного метода проводится попарное сравнение элементов нижележащих уровней иерархии относительно связанных элементов верхнего уровня иерархии. Для этого у каждой матрицы парных сравнений вычисляется собственный вектор и линейная свертка альтернатив приоритетов на иерархии [13].

При практическом использовании МАИ необходимо [10]:

1. выбрать порядок группировки;
2. выбрать шкалу экспертных оценок;
3. определить весовые коэффициенты каждого из уровней иерархии.
4. МАИ реализуется выполнением следующей последовательности действий [12]:

4.1. Определение проблемы и цели исследования (в решаемой задаче – выбор из множества возможных атак данного этапа

$$m_\alpha = \{m_{\alpha 1}, m_{\alpha 2}, \ldots m_{\alpha j}, \ldots m_{\alpha k}\}$$

наиболее вероятной атаки, которую будет использовать нарушитель, а также упорядочивание множества $M$ в соответствии с критериями, определяющими атаку).

4.2. Построение иерархии задачи с учетом целей атаки, этапов атаки и критериев, определяющих выбор данной атаки из существующих альтернатив (пример иерархической структуры задачи представлен на рис. 1).

4.3. Формирование на основе экспертных оценок, матрицы парных сравнений (МПС) на каждом этапе иерархии, начиная с нижних этапов

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{pmatrix},$$

где $a_{ij}$ – интенсивность появления $i$-го элемента иерархии относительно интенсивности $j$-го элемента иерархии, оцениваемая по шкале интенсивности от 1 до 9. При этом, если элемент $i$ важнее элемента $j$, значение $a_{ij}$ принимается равным значению интенсивности, выбранному экспертом, в противном случае, $a_{ij}$ принимается равным единице, деленной на данное число.


*Рис. 1. Пример иерархии задачи*
*(Fig. 1. Example of a hierarchy of tasks)*

4.4. Вычисление собственных чисел и собственных векторов матрицы $A$ и расчет на их основе векторов приоритетов и обобщенных весов атак.

4.5. Проверка согласованности МПС, составленных по результатам опросов различных экспертов, отклонение между которыми не должно превышать 20%.

Напомним, что метод МАИ допускает обобщение для случая, когда состояние исследуемой системы изменяется в течение времени, которое называется МАИ с динамическими приоритетами и предпочтениями [13]. В соответствие с данным методом на этапе 4.3 в моменты времени $t_1$ и $t_2$ получают две матрицы $A_1$, $A_2$, а на этапе 4.4, соответственно, два множества собственных чисел данных матриц – $\{\lambda_1\}$ и $\{\lambda_2\}$, что позволяет перейти от статических значений вероятностей, оцениваемых в различные последовательные моменты времени $t_1$ и $t_2$ к прогнозированию, например, с помощью линейной экстраполяции в момент времени $t_3$ значений множества $\{\lambda_3\}$. Применительно к рассматриваемой задаче знание значений множества $\{\lambda_3\}$, означает знание спрогнозированных в момент времени $t_3$ значений, по которым, в свою очередь, можно сделать прогноз динамических приоритетов и предпочтений выбранных векторов атак.

Результаты, подтверждающие работоспособность выбранного метода прогнозирования вероятностей компьютерных атак, обсуждаются в следующем разделе статьи.

## 3. Оценивание возможности прогнозирования вероятности компьютерных атак с помощью МАИ с динамическими приоритетами и предпочтениями

В связи с тем, что привлечь экспертов, количество которых обеспечило получение репрезентативных оценок МПС, оказалось невозможным, для составления МПС были использованы доступные статистические данные, в том числе: статистика инцидентов ИБ [14–16], результаты обсуждения способов эксплуатации уязвимостей на форумах DarkNet [17], данные Генпрокуратуры РФ [18] и новостных агрегаторов о громких делах в сфере ИБ.

По данным «Отчета Всемирного экономического форума по глобальным рискам» за 2018 г. [19] на финансовый сектор было совершено большее количество атак, чем на любой другой сектор экономики (17% от общего числа зарегистрированных атак). В этой связи для практического анализа применимости предложенного подхода были получены оценки вероятностей следующих векторов атак:

- целевые атаки на организации кредитно-финансового сектора (КФС);
- нецелевые (спам-атаки) на организации КФС;
- нецелевые атаки на клиентов КФС через зараженные популярные сайты;
- нецелевые атаки на клиентов КФС с использованием вирусного программного обеспечения (ВПО);
- нецелевые атаки на клиентов с использованием социальной инженерии.

При этом использовались ответы на следующие ключевые вопросы:

1) Какая из приведенных атак при однократной успешной реализации позволит похитить нарушителю наибольшую сумму денежных средств?

2) При использовании какой из атак наименьшая вероятность того, что нарушителя обнаружат, поймают и накажут в соответствии с законодательством РФ?

3) Какая из атак требует наименьшего времени на ее реализацию?

4) Способы реализации какой из атак более доступны?

При составлении МПС были использованы следующие показатели:

1) выгода атакующего в случае успешной реализации атаки (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать те типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

2) защита от преследования (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать такие типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

3) длительность атаки (при оценке по данному показателю следует выбирать наиболее быструю атаку, напомним, что по данным Лаборатории Касперского средняя продолжительность целевой атаки оставляет 100 дней [20]);

4) доступность методов для реализации атаки (при оценке по данному показателю будем учитывать оценивать доступность и известность технологии реализации атаки, наличие инструментов для реализации атаки в свободном доступе, а также активное обсуждение («объяснение») атаки на форумах DarkNet [17]).

Для подтверждения работоспособности предложенного подхода на основе доступных статистических данных за 2017 г. ($t_1$ = 2017 г.) и 2018 г. ($t_2$ =2018 г.), был

получен прогноз динамических приоритетов и предпочтений выбранных векторов атак в 2019 г. (момент времени $t_3$).

На этапе попарных сравнений по критерию «Выгода» была использована статистика, предоставленная 517-ю банками [14, 15], анализ которых показал, что полученная нарушителями выручка от целенаправленных атак составила:

– в 2017 г. – 50 млн. руб.;

– в 2018 г. – 4 млн. руб.;

количество целенаправленных атак:

– в 2017 г. – 39, из которых результативными оказались 22;

– в 2018 г. – 72 из которых результативными оказались 20.

Средняя выручка нарушителя от одной нецеленаправленной атаки, составлявшая в 2017 г. порядка 300$ (18 тыс. руб.) [21, 22], в 2018 г., по данным GroupIB, возросла до 40 тыс. руб. [16].

При оценке по показателю «защита от преследования» учитывались:

1) статистика Генпрокуратуры РФ [18] о количестве зарегистрированных преступлений:

– в 2018 г. – 121247;

– в 2017 г. – 90587,

2) результаты анализа статей новостного агрегатора о количестве громких судебных дел [16] в соответствие с которыми:

– в 2018 г. – из шести громких дел закончились арестом их фигурантов – 4;

– в 2017 г. – из четырех громких дел закончились арестом их фигурантов – 2;

3) данные ФинЦЕРТ [14, 15] о блокировке фишинговых ресурсов (ФинЦЕРТ начал эту работу с января 2017 года), в соответствие с которыми в периоды:

– 01.2017 – 08.2017: из 481 доменов, предложенных для разделегирования, разделегировано – 367;

– 09.2017 – 08.2018: из 2205 доменов, предложенных для разделегирования, разделегировано – 1668;

3) данные ФинЦЕРТ, в соответствие с которыми ФинЦЕРТ по блокировке номеров взаимодействовал:

– в 2017 г. – с тремя операторами связи;

– в 2018 г. – с семью операторами связи [14, 15].

При составлении МПС по показателю «доступность методов для реализации атаки» были использованы результаты исследований порядка 432060 постов форумов DarkNet [17], посвященных обсуждению методов атак.

Оценки весов показателей 2-го уровня иерархии, полученные авторами, представлены в табл. 1, 2.

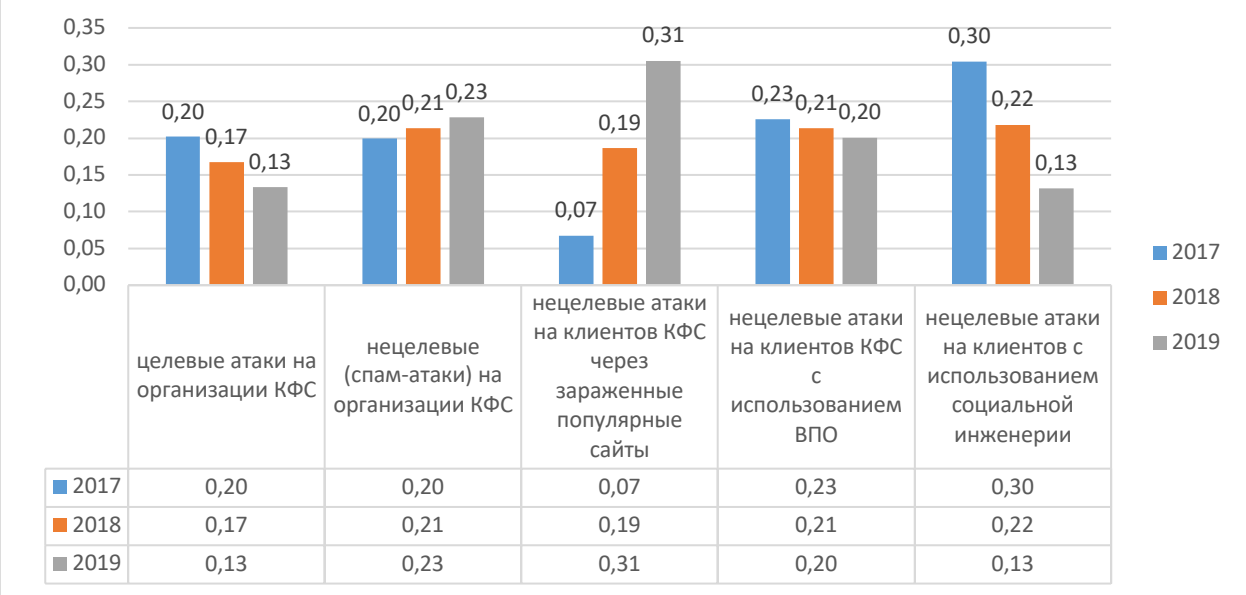
*Таблица 1. Итоговые результаты обобщенных весов атак за 2017 год*

| | Защита от преследования | Выгода | Доступность методов реакции на атаку | Длительность атаки | Обобщенные веса |
|---|---|---|---|---|---|
| веса критериев | 0,27 | 0,33 | 0,32 | 0,08 | – |
| целевые атаки на организации КФС | 0,02 | 0,57 | 0,02 | 0,03 | **0,20** |
| нецелевые (спам-атаки) на организации КФС | 0,13 | 0,29 | 0,17 | 0,17 | **0,20** |
| нецелевые атаки на клиентов КФС через зараженные популярные сайты | 0,12 | 0,03 | 0,05 | 0,11 | **0,07** |
| нецелевые атаки на клиентов КФС с использованием ВПО | 0,54 | 0,04 | 0,17 | 0,17 | **0,23** |
| нецелевые атаки на клиентов с использованием социальной инженерии | 0,19 | 0,08 | 0,58 | 0,53 | **0,30** |

*Таблица 2. Итоговые результаты обобщенных весов атак за 2018 год*

| | Защита от преследования | Выгода | Доступность методов реакции на атаку | Длительность атаки | Обобщенные веса |
|---|---|---|---|---|---|
| веса критериев | 0,27 | 0,27 | 0,27 | 0,19 | **–** |
| целевые атаки на организации КФС | 0,14 | 0,26 | 0,13 | 0,14 | **0,17** |
| нецелевые (спам-атаки) на организации КФС | 0,20 | 0,22 | 0,22 | 0,21 | **0,21** |
| нецелевые атаки на клиентов КФС через зараженные популярные сайты | 0,20 | 0,15 | 0,19 | 0,20 | **0,19** |
| нецелевые атаки на клиентов КФС с использованием ВПО | 0,25 | 0,18 | 0,22 | 0,21 | **0,21** |
| нецелевые атаки на клиентов с использованием социальной инженерии | 0,21 | 0,19 | 0,24 | 0,24 | **0,22** |

Оценки вероятностей атак в 2017 г. и 2018 г. и спрогнозированные значения вероятностей атак в 2019 г. представлены на рис. 2.




| | целевые атаки на организации КФС | нецелевые (спам-атаки) на организации КФС | нецелевые атаки на клиентов КФС через зараженные популярные сайты | нецелевые атаки на клиентов КФС с использованием ВПО | нецелевые атаки на клиентов с использованием социальной инженерии |
|---|---|---|---|---|---|
| 2017 | 0,20 | 0,20 | 0,07 | 0,23 | 0,30 |
| 2018 | 0,17 | 0,21 | 0,19 | 0,21 | 0,22 |
| 2019 | 0,13 | 0,23 | 0,31 | 0,20 | 0,13 |

*Рис. 2. Фактические значения вероятностей атак, вычисленные по статистическим данным за 2017 г., 2018 г., и прогнозируемые значения на 2019 г.*
*(Fig. 2. Actual values of attack probabilities calculated using the statistics for 2017, 2018, and predicted values for 2019)*

### 4. Оценка адекватности спрогнозированных значений вероятностей атак

В связи с тем, что в отчете Банка России [23] представлены не количественные значения показателей атак, а только качественные описания фактических векторов атак, проведено сравнение спрогнозированной динамики изменений вероятности атак с аналогичными данными, представленными в отчете.

Результаты сравнения показывают, что прогноз динамики изменения векторов атак оказался верным у:

– целевых атак на организации КФС;
– нецелевых атак (спам-атаки) на организации КФС;
– нецелевых атак на клиентов КФС через зараженные популярные сайты;
– нецелевых атак на клиентов КФС с использованием вирусного программного обеспечения (ВПО).

Эти выводы также подтверждаются тем, что в 2019 г. [23]:

1. произошло смещение фокуса внимания злоумышленников с организаций кредитно-финансового сектора на их клиентов (88% данных для реализации нецелевых атак на клиентов КФС нарушители получают через зараженные сайты, «продающие какие-либо товары или оказывающие какие-либо услуги с дистанционной оплатой с использованием карт», а также торговые площадки);
2. вредоносное программное обеспечение по-прежнему остается одним из основных инструментов компьютерных преступников.

Динамика спрогнозированной в работе вероятности атаки, связанного с социальной инженерией, отличается от фактической, так как не был предсказан появившийся в 2019 г. в арсенале злоумышленников новый способ обмана жертв (подмена исходящего телефонного номера на номер КФО и выдача себя за сотрудника безопасности банка) [23].

Обнаруженное расхождения спрогнозированных и фактических результатов свидетельствует о некорректном оценивании динамического набора альтернатив [25],

обусловленное тем, что показатель «доступность методов для реализации атаки» оценивался по данным, представленным на форумах DarkNet [17], в то время как нарушители ИБ также используют методы социальной инженерии, выходящие за рамки информационных технологий (например, телефонное мошенничество [24]).

## Заключение

В статье обоснована возможность динамического оценивания вероятности угроз информационной безопасности с позиции нарушителя на основе использования метода анализа иерархий с динамическими приоритетами и предпочтениями.

Получены оценки вероятностей компьютерных атак и векторов атак на основе доступной статистики о компьютерных атаках за 2017–2018 гг., а также сделан соответствующий прогноз на 2019 г.

Проведена оценка адекватности прогнозирования вероятности компьютерных атак на 2019 г., свидетельствующая о правильности прогнозирования динамики изменения векторов атак на организации кредитно-финансового сектора: целевых атак, нецелевых атак (спам-атак); нецелевых атак на клиентов КФС через зараженные популярные сайты, также с использованием вирусного программного обеспечения.

Обнаружено расхождение спрогнозированного и фактического значения вероятности атаки, связанной с социальной инженерией, что свидетельствует о необходимости дальнейших исследований с целью уточнения приоритетов и моделей поведения нарушителей ИБ в конкретной отрасли и организации.

СПИСОК ЛИТЕРАТУРЫ:

1. В РЖД заявили о небольшом ущербе от атаки вируса WannaCry // INTERFAX.RU/ URL: https://www.interfax.ru/russia/563900/ (дата обращения: 17.11.2019).
2. Трунина А., Рождественский И., Фадеева А., Вовнякова А. «Роснефть» сообщила о мощной хакерской атаке на свои серверы // URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c/ (дата обращения: 17.11.2019).
3. Чернышова Е., Фейнберг А. Сбербанк назвал версии утечки данных своих клиентов // URL: https://www.rbc.ru/finances/03/10/2019/5d960ab29a79471ea76e1769/ (дата обращения: 17.11.2019).
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). М.: ФСТЭК России, 2008. – 69 с.
5. Приказ № 17 от 11 февраля 2013 г. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. М.: ФСТЭК России, 2013. – 39 с.
6. Банк данных угроз безопасности информации ФСТЭК России // FSTEC.RU/ URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2019).
7. Международный стандарт ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 с.
8. Threat Zone'19. Иллюзия безопасности. BiZone. 140 с.
9. Erdoğan M., Karaşan A., Kaya I., Budak A., Çolak M. A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies // Материалы «International Conference on Intelligent and Fuzzy Systems», INFUS 2019, Istanbul, Turkey, 23 – 25 июля 2019. С. 1042–1049.
10. Микони С.В. Теория принятия управленческих решений. СПб: Лань, 2015. – 448 с.
11. Черноруцкий И. Г. Методы принятия решений // СПб.: Петербург. 2005. – 416 с.
12. Насыров Р.В., Тайгина Е.А., Фарукшин Р.М. Применение метода анализа иерархий в практике научных исследований // Управление в сложных системах. 1999. С. 101–107.
13. Андрейчиков А. В., Андрейчикова О. Н. Методы и интеллектуальные системы принятия решений для проведения ФОРСАЙТ-исследований // Электронный журнал Cloud of Science. 2014. Т. 1. № 3. С. 353–380.
14. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2017 – 31.08.2018 // CRB.RU/ URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (дата обращения: 17.11.2019).

15. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году // CRB.RU/ URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (дата обращения: 17.11.2019).
16. Потери банков от киберпреступности // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/ Статья: Потери_банков_от_киберпреступности / (дата обращения: 17.11.2019).
17. Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment // Information. 9 (11). 2018. – 18 с.
18. Киберпреступность и киберконфликты // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/ Статья:Киберпреступность_и_киберконфликты_:_Россия/ (дата обращения: 17.11.2019).
19. The Global Risks Report 2018 // MARSH&McLENNAN COMPANIES. Выпуск 13. 2018. – 80 с.
20. Анатомия таргетированной атаки // KASPERSKY.RU/ URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 17.11.2019).
21. За два дня хакеры заработали на вирусе Petya 4 биткоина // RBC.RU/ URL: https://www.rbc.ru/technology_and_media/28/06/2017/5953f1059a7947672bb08f33?from=newsfeed/ (дата обращения: 17.11.2019).
22. Вирус-шифровальщик едва окупается // VEDOMOSTI.RU/ URL: https://www.vedomosti.ru/technology/articles/2017/06/29/700968-virus-shifrovalschik-okupaetsya/ (дата обращения: 17.11.2019).
23. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019 // CRB.RU/ URL: https://www.cbr.ru/content/document/file/84354/fincert_report_20191010.pdf/ (дата обращения: 17.11.2019).
24. Здор В. Методы социальной инженерии // bis-expert.ru / URL: https://bis-expert.ru/blog/2046/6950/ (дата обращения: 17.11.2019).
25. Колесникова С.И. Модификация метода анализа иерархий для динамических наборов альтернатив // Прикладная дискретная математика №4 (6). 2009. С. 102–109.

REFERENCES:

[1] The Russian Railways claimed little damage from the attack of the WannaCry virus. INTERFAX.RU URL: https://www.interfax.ru/russia/563900/ (accessed: 17.11.2019) (in Russian).
[2] Trunina A., Rozhdestvensky I., Fadeeva A., Vovnyakova A. Rosneft reports a powerful hacker attack on its servers. URL: https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c/ (accessed: 17.11.2019) (in Russian).
[3] Chernyshova E., Feinberg A. Sberbank named the version of data leakage of its customers. URL: https://www.rbc.ru/finances/03/10/2019/5d960ab29a79471ea76e1769/ (accessed: 17.11.2019) (in Russian).
[4] Basic model of personal data security threats. M.: FSTEC of Russia, 2008. – 69 p. (in Russian).
[5] Order № 17 11.02.2013. On the approval of information security requirements that are not a state secret are provided in state information systems. M.: FSTEC of Russia, 2013. – 39 p. (in Russian).
[6] Databank of information security threats of the FSTEC of Russia. FSTEC.RU URL: https://bdu.fstec.ru/ (accessed:17.11.2019) (in Russian).
[7] International Standard ISO/IEC 27001: 2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p.
[8] Threat Zone'19. The illusion of security. BiZone. 140 p.
[9] Erdoğan M., Karaşan A., Kaya I., Budak A., Çolak M. A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies. Materials of the International Conference on Intelligent and Fuzzy Systems, INFUS 2019, Istanbul, Turkey, July 23 – 25, 2019. P. 1042–1049.
[10] Mikoni S.V. Theory of managerial decision making. St. Petersburg: Lan, 2015. – 448 p. (in Russian).
[11] Chernorutsky I.G. Decision Making Methods. St. Petersburg: Petersburg. 2005. – 416 p. (in Russian).
[12] Nasyrov R.V., Taigina E.A., Farukshin R.M. Application of the method of analysis of hierarchies in the practice of scientific research. Management in complex systems. 1999. P. 101–107 (in Russian).
[13] Andreichikov A.V., Andreichikova O. N. Methods and intelligent decision-making systems for conducting FORSIGHT research. Electronic journal Cloud of Science. 2014. T. 1. No. 3. P. 353–380. (in Russian).
[14] Report of the Center for Monitoring and Response to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia 1.09.2017 – 08.31.2018. CRB.RU URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (accessed: 17.11.2019) (in Russian).

[15] Overview of the main types of computer attacks in the financial sector in 2018. CRB.RU URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (accessed: 11.17.2019) (in Russian).
[16] Losses of banks from cybercrime. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Losses_of_banks_from cybercrime (accessed: 17.11.2019) (in Russian).
[17] Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment. Information. 9 (11) 2018. – 18 p.
[18] Cybercrime and cyberconflicts. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Cybercrime_and_kiberconflicts_:_Russia/ (accessed: 17.11.2019) (in Russian).
[19] The Global Risks Report 2018. MARSH&McLENNAN COMPANIES. Edition 13. 2018. – 80 p.
[20] Anatomy of a targeted attack. KASPERSKY.RU URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (accessed: 17.11.2019) (in Russian).
[21] In two days, hackers earned 4 bitcoins on Petya virus. RBC.RU URL: https://www.rbc.ru/technology_and_media/28/06/2017/5953f1059a7947672bb08f33?from=newsfeed/ (accessed: 17.11.2019) (in Russian).
[22] The encryption virus is barely paying off. VEDOMOSTI.RU URL: https://www.vedomosti.ru/technology/articles/2017/06/29/700968-virus-shifrovalschik-okupaetsya/ (accessed: 17.11.2019) (in Russian).
[23] Report of the Center for Monitoring and Response to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia 1.09.2018 - 08.31.2019. CRB.RU URL: https://www.cbr.ru/content/document/file/84354/fincert_report_20191010.pdf/ (accessed: 17.11.2019) (in Russian).
[24] Zdor V. Methods of social engineering. bis-expert.ru URL: https://bis-expert.ru/blog/2046/6950/ (accessed: 17.11.2019) (in Russian).
[25] Kolesnikova S.I. Modification of the hierarchy analysis method for dynamic sets of alternatives. Applied Discrete Mathematics №4 (6). 2009. P. 102–109 (in Russian).

*Поступила в редакцию – 02 декабря 2019 г. Окончательный вариант – 04 февраля 2020 г.*
*Received – December 02, 2019. The final version – February 04, 2020.*