Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

На правах рукописи

Макарова Ольга Сергеевна

РАЗРАБОТКА МЕТОДИКИ ПРОГНОЗИРОВАНИЯ ДИНАМИКИ ИЗМЕНЕНИЯ ВЕКТОРА КОМПЬЮТЕРНОЙ АТАКИ С ТОЧКИ ЗРЕНИЯ НАРУШИТЕЛЯ

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Екатеринбург – 2021

Работа выполнена в учебно-научном центре «Информационная безопасность» Института радиоэлектроники и информационных технологий-РтФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина».

Научный руководитель: доктор технических наук, профессор
ПОРШНЕВ Сергей Владимирович

Официальные оппоненты: **КОЗАЧОК Александр Васильевич**, доктор технических наук, доцент, ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», г. Орёл, сотрудник Академии ФСО России;

БАРАНКОВА Инна Ильинична, доктор технических наук, доцент, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск, заведующий кафедрой информатики и информационной безопасности;

ЗЫРЯНОВА Татьяна Юрьевна, кандидат технических наук, ФГБОУ ВО «Уральский государственный университет путей сообщения», г. Екатеринбург, доцент кафедры «Информационные технологии и защита информации»

Защита диссертации состоится «21» декабря 2021 г. в 11:00 часов на заседании диссертационного совета УрФУ 2.3.05.13 по адресу: 620002, г. Екатеринбург, ул. Мира, 19, ауд. И-420 (зал Ученого совета).

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»: https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=3050

Автореферат разослан «__._» _____ 2021 года.

Ученый секретарь
диссертационного совета Сафиуллин Николай Тахирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования и степень ее проработанности.

Защита информации (ЗИ) предусмотрена Статьей 16 Федерального закона (ФЗ) от 27.07.2006 «Об информации, информационных технологиях и о защите информации», а также иными нормативно-правовыми актами, разработанными государственными регуляторами в области информационной безопасности (ИБ), в том числе, в сфере защиты критической информационной инфраструктуры. Данные документы предусматривают применение типовых наборов методов и средств ЗИ, сформированных на базе типовых моделей угроз ИБ, созданных ФСТЭК России и ФСБ России. При этом действующим законодательством предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми. В соответствие с «Методикой оценки угроз безопасности информации», разработанной ФСТЭК России, оценка угроз ИБ осуществляется с помощью метода экспертных оценок.

Международные стандарты в области ЗИ рекомендуют использовать те или иные известные методологии, каждая из которых, де-факто, базируются на:

– методологии *IT-Grundschutz*, которая, в одних случаях, рекомендует использовать в организациях и информационных системах набор мер ЗИ, состав которого определен на основе сценариев негативных последствий для активов организации, а в других, также применять дополнительный перечень мер ЗИ, формируемый экспертным путем;

– методологии *ISO* 2700x, предусматривающую формирование набора требований по ЗИ на основе оценки рисков ИБ, которая в соответствии с внутренним положением организации по оценке рисков ИБ осуществляется экспертным путем. При этом ответственность за принятие рисков в целом несет руководитель организации (владелец активов).

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

В этой связи были предприняты многочисленные попытки модернизации действующих международных и российских стандартов и нормативно-правовых документов в области обеспечения ИБ с целью автоматизации процесса формирования профилей ЗИ, использования соответствующих инструментов, обеспечивающих их наглядную визуализацию, а также специальных методов ее проведения, которые в ряде случаев могут повысить эффективность экспертной оценки, представленные в работах как российских исследователей Финогеева А. А., Финогеева А. Г., Нефедовой И. С., Белокуровой Е.В., Дерканосовой А.А., Змеева А.А., Сидельникова А.П, Коробейникова А.Г., Гришенцева А.Ю., Комарова И.Э., Ашевского Д.Ю., Алексанина С.А., Маркиной Г.Л., Козина И. С., так и зарубежных *MacDonald D., Clements S.L., Patrick S.W., Perkins C., Muller G., Lancaster M.J., Hutton W., Abdo H. A, Casola V., Bracho. A. A., Zhang W.* При этом

оценка угроз и рисков ИБ в данных работах проводились, исключительно, с точки зрения организации/владельца актива, кроме того в большинстве этих работ их авторы не пытались оценить эффективность и практическую применимость, предложенных ими изменений.

Также необходимо отметить, работы *Seul-Ki Choi, Taejin Lee, Jin Kwak, Bo Feng, Qiang Li , Yuede Ji , Dong Guo* (Китай), *Deb A., Lerman K., Ferrara E.* (США), 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 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 методах проведения КА при оценке угроз ИБ, которые, однако, не завершились созданием рекомендаций по оценке целесообразности проведения КА с точки зрения нарушителя. В этой связи использование информации, извлекаемой с форумов *DarkNet,* для прогнозирования векторов КА оказалось низким.

Использование классических методов одинарного, двойного и тройного экспоненциального сглаживания, статистических методов (Кростона, *ARIMA*), кластерного анализа, нейронных сетей и машинного обучения, в работах зарубежных исследователей *Yasasin. E., Xiong. J., Wu J., Pokhrel, N.R., Rodrigo, H., Tsokos, C.P., Nwankpa, J.K., Roumani, Y.F., Movahedi, Yazdan, Cukier, M., Andongabo, A., Gashi, I.* при прогнозировании как новых уязвимостей ПО в обновленных версиях ПО (ОС, браузерах, офисных приложениях и др.), основанных на анализе накопленной информации о количестве уязвимостей и их типах в их предыдущих версиях, так и вектора КА, основанных на анализе частоты упоминаний методов КА за определенные временные периоды (в работах *Deb A., Lerman K., Ferrara E.*), оказалось не эффективным, так как расходилось с реальными данными.

В тоже время в экономической и финансовой 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, которая, однако, при оценке вероятностей КА ранее не использовалась. В этой связи разработка подходов по оценке угроз ИБ с учетом экономических интересов нарушителя является актуальной.

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

Для достижения поставленной цели 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 выражается в:

1. 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 в:

1. 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.

Основные положения, выносимые на защиту

1. Разработана математическая модель принятия решения нарушителем о проведении КА, основанная на ТПК, и подтверждена ее адекватность результатами: натурного моделирования КА с помощью программно-аппаратного комплекса «*Ampire*» (ПАК «*Ampire*»); анализа КА, реализованной с помощью вредоносного программного обеспечения (ВПО) *Petya;* прогнозирования целевых и нецелевых КА, полученными на основе использования информации о более чем 700 тысячах обнаруженных КА (анализа КА, реализуемых через заражение популярных сайтов; анализа КА, реализуемых с использованием вредоносного

программного обеспечения (ВПО) или социальной инженерии на организации кредитно-финансового сектора (КФС)).

2. Разработана математическая модель динамики распространения КА, основанная на использовании ТПК и Теории диффузии инноваций (ТДИ), и подтверждена ее адекватность результатами: 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 КФС.

3. Разработана методика прогнозирования динамики вектора КА, основанная на использовании математической моделей принятия решения нарушителем о проведении КА и математической модели, описывающей динамику распространения КА, адекватность которой подтверждена непротиворечивостью результатов спрогнозированного вектора КА в 2019 г. с соответствующими результатами анализа доступной статистической информации об успешно реализованных КА.

Достоверность полученных результатов обеспечивается использованием 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 ПАК «*Ampire*».

Внедрение результатов диссертационного исследования. Результаты диссертационного исследования используются в федеральном государственном автономном образовательном учреждении высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (акт об использовании № 33.02-32/230 от 20.08.2021), Акционерном обществе «Перспективный мониторинг» (акт об использовании № ИПМ-2021-0104 от 23.08.2021).

Апробация работы. Основные результаты работы докладывались на следующих научных конференциях: III международной студенческой научной конференции «Инновационные механизмы управления цифровой и региональной экономикой», 17.06-18.06.2021, Москва, 2021; международной научной конференции Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 13.05-14.05.2021, Екатеринбург, USBEREIT, 2021; международной научно-технической конференции «Автоматизация», 6.09-12.09.2020, Сочи, 2020; международной научной конференции Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 14.05-15.05.2020, Екатеринбург, 2020; I международной научной конференции «Технические науки: проблемы и перспективы», март 2011, Санкт-Петербург, 2011.

Личный вклад. Автор обосновал возможность прогнозирования динамики вектора КА с точки зрения нарушителя во времени на основе данных из общедоступных источников информации о КА получив практически подтвержденные результаты оценки. Разработал научно обоснованные

математические модели определения ожидаемой полезности от КА и динамики возможности реализации КА во времени с точки зрения нарушителя.

Публикации. По теме диссертации опубликовано 10 научных работ, в том числе 6 научных статей в изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, из них 2 статьи в изданиях, индексируемых в международных цитатно-аналитически базах *Scopus*.

Объем и структура работы. Диссертация состоит из введения, 3 глав, заключения и 8 приложений. Полный объем диссертации составляет 218 страниц, включая 26 рисунков и 25 таблиц. Список литературы содержит 178 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность выбранной темы исследования, сформированы цель и задачи исследования, а также основные научные результаты диссертации и ее краткое содержание. Приводятся основные положения, выносимые на защиту, сформулирована научная новизна, теоретическая и практическая значимость проведенного исследования.

Первая глава посвящена анализу предметной области, в том числе анализу нормативно-правовой базы РФ, 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 динамики вектора 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, ИТ-подходы к выявлению уязвимостей, ТПК, в которой учитывается экономическая мотивация совершаемого преступления и ТДИ.

В соответствие с ТПК любой человек, потенциально, может стать нарушителем при выполнении следующих условий:

1. Наличия возможности совершения преступления.
2. Получения в случае совершения преступления достаточной (с точки зрения нарушителя) полезности.

В этой связи, сделан обоснованный вывод о том, что математическая модель КА должна включать в себя:

– математическую модель принятия решения нарушителем о проведении КА, в которой учтены мотивы нарушителя и принципы принятия решения о проведении/продолжении/прекращении КА;

– математическую модель развития КА во времени, включающую в себя критерии выбора объекта КА нарушителем, этапы и методы реализации КА, методы получения информации об объекте.

Принимая во внимание, условие совершения преступления, сформулированное в ТПК («если ожидаемая полезность от преступления превышает полезность от иной деятельности, на которую были бы затрачены те же силы и время, то нарушитель совершит преступление») предложено оценивать вероятность реализации КА вида «А», реализуемой нарушителем, как условную вероятность достаточности ожидаемой полезности КА при наличии возможности проведения КА, рассчитываемую по формуле:

$$P(EUA) = P(EU|A)\ \mathrm{P}(A),$$

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 проведения КА.

Для расчета условной вероятности ожидаемой полезности КА вида «*A*» с точки зрения нарушителя, при оценивании которой учитывается возможность проведения КА, предложено определять вероятность достаточности ожидаемой полезности КА вида «*A*» с точки зрения нарушителя по формуле:

$$P(EU|A) = \frac{EU_A}{EU_\Sigma},$$

где

EU_A – ожидаемая полезность КА вида «А» с точки зрения нарушителя, при оценивании которой учитывается возможность проведения КА;

$EU_\Sigma = \sum_{j=1}^{J} EU_j$ – ожидаемая полезность с учетом всех доходов нарушителя, при оценивании которой учитывается возможность проведения КА, j – порядковый номер метода КА, использованного нарушителем.

Для определения ожидаемой полезности КА вида «А» с точки зрения нарушителя разработана математическая модель принятия решений нарушителем о проведении КА, представляющая собой функцию ожидаемой полезности, используемую в ТПК, модернизированную с учетом описанных выше особенностей КА и преступлений в информационной сфере:

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

где $U(\xi)$ – функция полезности,

ρ_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной КА $\rho_m = 1-\rho_n$).

W_m – выгода нарушителя в случае успешной реализации КА,

W_j – текущий доход нарушителя от легальной деятельности,

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

В связи с тем, что нарушитель, как правило, является среднестатистическим человеком, по оценке Бернулли, не склонным к риску, в качестве функции полезности $U(\xi)$, следуя ТПК выбрана функция,

$$U(\xi) = b\ln\left(\frac{a+\xi}{a}\right),$$

где a, b – константы.

Анализ формулы вероятности ожидаемой полезности КА показал, что без ограничения общности, в функции полезности параметры a, b можно принято равными следующим значениям: b=1, a=МРОТ (с целью наглядности графиков).

Далее проведен анализ и обоснован выбор источников первичной информации, необходимой для вычисления оценок параметров КА, приведенных выше, и предложено использовать для расчета вероятности проведения незаметной КА результаты анализа статей новостного агрегатора о количестве громких судебных дел, а также статистику Генпрокуратуры РФ о количестве зарегистрированных преступлений (см. *http://www.tadviser.ru/index.php/*) и данные ФинЦЕРТ о блокировке фишинговых ресурсов и телефонных номеров (см. *https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/*, *https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/*). Приведен пример вычисления оценки вероятности принятия решения преступником о проведении КА с использованием ВПО *Petya*. В третьей главе проведен анализ более 30 возможных источников общедоступной информации.

При построении математической модели, описывающей динамику возможности реализации КА принято во внимание, что на этапе подготовки к реализации нарушителем КА вида «А» нарушитель стремится получить сведения о новых для него технологиях, проведения КА, то есть инновациях. Инновация – технологическая идея, метод или объект, являющийся новым для члена социальной системы. В этой связи для определения вероятности наличия возможности реализации нарушителем КА вида «А» предложено использовать ТДИ (здесь диффузия инноваций – это процесс, с помощью которого инновации распространяются по каналам передачи с течением времени среди членов социальной системы), развитой в Э. Роджерсом, Ф. Бассом, Э. Мэнсфилдом и Т. Хагерстранда. В соответствие с ТДИ процесс распространения инноваций описывается s-образными кривыми Перла-Рида – функциями вида:

$$P(A,t) = \frac{1}{1+\alpha e^{-\beta t}},$$

где α, β – параметры модели оценки вероятности возможности реализации нарушителем КА вида «А», а t – безразмерная величина, определяемая по формуле $t = \frac{T - T_0}{месяц}$.

При каскадом (поэтапном) проведении КА динамика распространения КА описывается функцией:

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

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 внедрения инновации.

Обосновано, что в терминах КА диффузия – это процесс, с помощью которого информация о методе реализации КА распространяется по каналам передачи с течением времени среди нарушителей.

В терминах КА процесс принятия решения о возможности использования метода КА проходит пять этапов:

1. Знание – нарушитель (или другое устройство по принятию решений) узнает об методе КА и понимает, как он реализуется.

2. Убеждение – нарушитель формирует представление о преимуществах и недостатках метода КА.

3. Принятие решения – нарушитель принимает решение о применимости метода КА (принимает или не принимает к использованию).

4. Применение – нарушитель использует КА. На этом этапе идет адаптация (проверка) метода КА.

5. Подтверждение – нарушитель принимает решение о дальнейшем использовании метода КА.

Таким образом, возможность реализации КА зависит как от знаний и умений нарушителя – (три первых этапа), так и от практической возможности реализовать КА в инфраструктуре организации, являющейся объектом КА (четвертый и пятый этапы). Соответственно, для разработки научно обоснованных рекомендаций по идентификации параметров математической модели, описывающей динамику КА, выделены обобщенные этапы реализации КА с точки зрения нарушителя:

1. Этап теоретической подготовки, включающий в себя этапы, связанные с изучением объекта КА и подготовкой к КА.

2. Этап практической подготовки, включающий в себя, связанные с практической реализации подготовительной части КА.

3. Этап достижение цели КА, включающий в себя практическую реализацию цели КА, в том числе, причинение вреда.

Выделенные этапы сопоставлены с существующими подходами к определению этапов КА: *Cyber Kill Chain, NIST 800-115, Certified Ethical Hacker*, и не противоречат им, а структурируют и упрощают.

Адекватность построенной математической модели проведения КА подтверждена с помощью натурного моделирования на ПАК «Ampire» и результатами анализа архивных данных о динамике изменения количества зараженных узлов во время проведения КА ВПО *WannaCry*, размещенных на сайте *MalwareTech*.

1. Результаты определения значений коэффициентов аппроксимирующих функций архивных данных о динамике изменения количества зараженных узлов во время проведения КА ВПО *WannaCry*, а также остатки данных моделей представлены в таблице Таблица 1.

Таблица 1. Значения коэффициентов аппроксимирующих функций

Тип функции	α_1	α_2	α_3	α_4	Дисперсия остатков модели
Линейная	0,00041	–0.073	–	–	0.065
Квадратическая	$-5\cdot10^{-8}$	0,00056	–0.15	–	0.053
s-образная	–0.11025	1.18080	0.00197	13.7642	0.021

Значения коэффициентов линейной и квадратической аппроксимирующих функций, а также s-образной кривой Перла-Рида, находились, соответственно, из условий:

$$\arg\min_{\alpha_1,\alpha_2}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i+\alpha_2\right)\right)\right)^2,$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i^2+\alpha_2 t_i+\alpha_3\right)\right)\right)^2,$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1+\frac{\alpha_2}{1+\alpha_3\exp\left(-\left(\alpha_4\left(t_i-t_1\right)\right)\right)}\right)\right)\right)^2,$$

N – число отсчетов аппроксимируемой зависимости. Для нахождения решения первых двух задач использовалась функция пакета *MATLAB regress.m*, третьей задачи – функция *fminsearch.m*.

2. Результаты натурного моделировании КА на программно-аппаратном комплексе, разработанном для обучения методам обнаружения, анализа и устранения последствий КА «*Ampire*», представленными на рисунке 1.

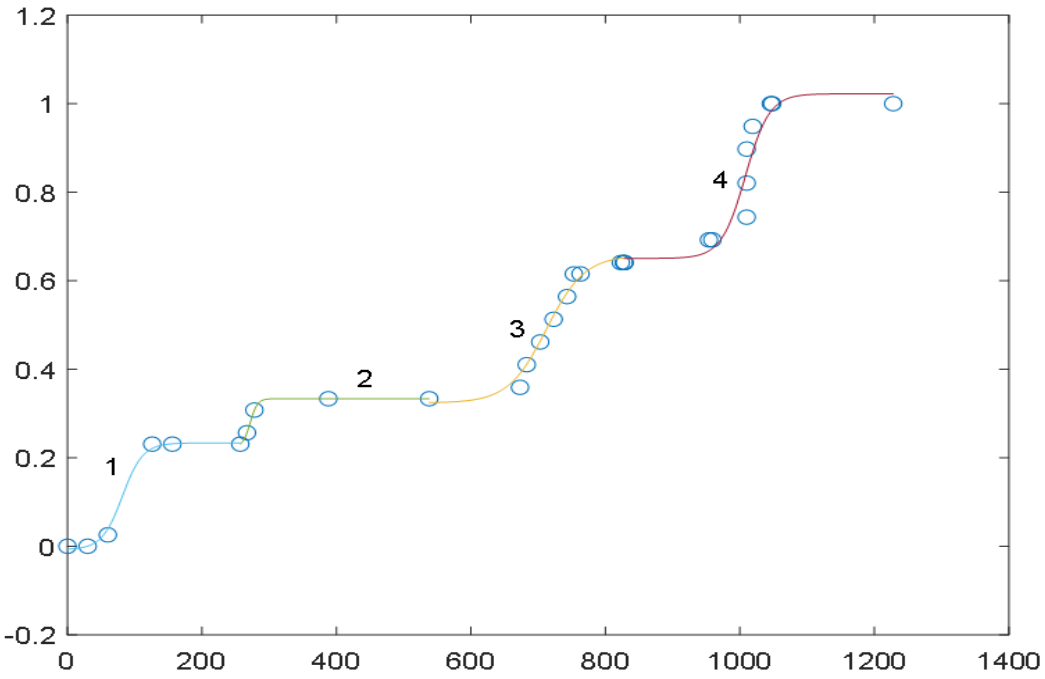

Рисунок 1. Результаты интервальной аппроксимации зависимости относительного числа зараженных узлов от времени, эквивалентной зависимости вероятности возможности реализации методов КА от времени

Аппроксимирующая функция представляет собой набор s-образных кривых Перла-Рида, заданных на последовательных интервалах. На каждом из выбранных временных интервалов в соответствие с методом наименьших квадратов были вычислены параметры s-образных кривых Перла-Рида, аппросимировавшиеся на выбранных временных интервалах функциями

$$y_k(t) = \alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3 e^{-\alpha_4^k \left(t - t_0^{\langle k \rangle}\right)}},$$

где

$k = \overline{1,4}$ – номер интервала аппроксимации.

Значения коэффициентов аппроксимирующих функций $\alpha_j^{\langle k \rangle}$, $j = \overline{1,4}$ находились из условия:

$$\underset{\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}}{\arg} \min \left(\sum_{i=1}^{N^{\langle k \rangle}} \left(y_i - \left(\alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3^{\langle k \rangle} \exp\left(-\left(\alpha_4^{\langle k \rangle} \left(t_i - t_1 \right) \right) \right)} \right) \right) \right)^2,$$

где

$N^{\langle k \rangle}$ – число отсчетов аппроксимируемой зависимости, укладывающихся на k-ом интервале, с помощью функции пакета *MATLAB fminsearch.m*.

Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k\rangle},\alpha_2^{\langle k\rangle},\alpha_3^{\langle k\rangle},\alpha_4^{\langle k\rangle}$, представлены в таблице.

Таблица 2. Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k\rangle},\alpha_2^{\langle k\rangle},\alpha_3^{\langle k\rangle},\alpha_4^{\langle k\rangle}$ аппроксимирующих функций

k	Начальное приближение				Значения коэффиентов			
	$\alpha_1^{\langle k\rangle}$	$\alpha_2^{\langle k\rangle}$	$\alpha_3^{\langle k\rangle}$	$\alpha_4^{\langle k\rangle}$	$\alpha_1^{\langle k\rangle}$	$\alpha_2^{\langle k\rangle}$	$\alpha_3^{\langle k\rangle}$	$\alpha_4^{\langle k\rangle}$
1	0	0,1	1,0	200,0	–0.0076	0.2409	0.0658	216.6173
2	0,2308	0,1	1,0	400,0	0.2241	0.10925	0.1862	15.3182
3	0,3333	0,1	5,0	10,0	0.3237	0.33365	0.0353	466.8322
4	0,6410	0,1	1,0	40,0	0.6503	0,3720	0,0560	23712.73138

Предложен и обоснован подход к определению параметров на этапе теоретической подготовки, включающий в себя этапы, связанные с изучением объекта КА и подготовкой к КА, основанный на использовании модели Мэнсфилда, в соответствие с которой α определяется:

– рентабельностью использования этого метода КА по сравнению с альтернативными методами (характеризуется W_m – выгода нарушителя в случае успешной реализации КА, W_j – текущий доход нарушителя от легальной деятельности, F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте));

– инвестициями, необходимые для реализации метода КА (стоимостью C_j метода в сетях *DarkNet* относительно других методов), в процентах от средней общей суммы активов нарушителя, определяемой стоимостью метода КА.

В этой связи оценку параметра α предложено вычислять по формуле:

$$\alpha_j = \frac{\left(1-\rho_{nj}\right)\left(W_{mj}+W_j\right)+\rho_{nj}\left(W_{mj}+W_j-F_j\right)}{W_{mj}-C_j}$$

где

j – рассматриваемый метод КА;

ρ_{nj} – вероятность разоблачения нарушителя;

C_j – стоимость КА в сетях *DarkNet*;

W_i – текущий доход нарушителя от легальной деятельности;

W_{mj} – доход нарушителя от реализации j-ого метода КА;

В соответствии с моделью Басса параметр β, на теоретическом этапе характеризуется:

– рекламой в *DarkNet* с целью приобретения/использования рассматриваемого метода КА (определяется на первом этапе КА). В соответствии с моделью Басса для новых методов КА это в первую очередь реклама – количество упоминаний в сетях *DarkNet* (известность метода КА в сети *DarkNet* a_n).

– данными межличностного взаимодействия нарушителей в *DarkNet*, которые уже приобрели/использовали рассматриваемый метод КА (определяется

на втором этапе КА) a_l и практической апробацией метода КА a_p – совместимость с инфраструктурой атакуемой организации, сложностью реализации, появлением подтверждений применения/наказания при использовании данного метода КА в сети *DarkNet*, новостных агрегаторах, свой опыт тестирования.

$$\beta_j = a_n + a_l + a_p,$$

где

j – рассматриваемый метод КА;

a_n – известность метода КА в сети *DarkNet*;

a_l – коэффициент межличностной рекламы метода КА в *DarkNet* (успешности реализации аналогичных КА),

a_p – коэффициент апробации метода КА в *DarkNet* (успешная практическая проверка метода КА), оцениваемый на основе данных новостных агрегаторов и/или данных центров мониторинга ИБ.

Корректность определения параметров α, β подтверждена результатами анализа КА, реализованной с помощью ВПО *Petya* в период с апреля 2016 по июль 2017 гг. на узлы компьютерной сети Украины. Анализ динамики проведения данной КА позволил сделать обоснованный вывод о том, что вероятность возможности реализации КА ВПО *Petya* существенно возросла после ее успешного тестирования в апреле 2016 г. (реализации широкомасштабной КА ВПО *WannaCry*), зависимость которой от времени в период с мая по сентябрь 2017 г. и далее описывается функцией

$$Y(t) = \frac{1}{1 - 1{,}05e^{-212t}},$$

график которой представлен на рисунке *1*.

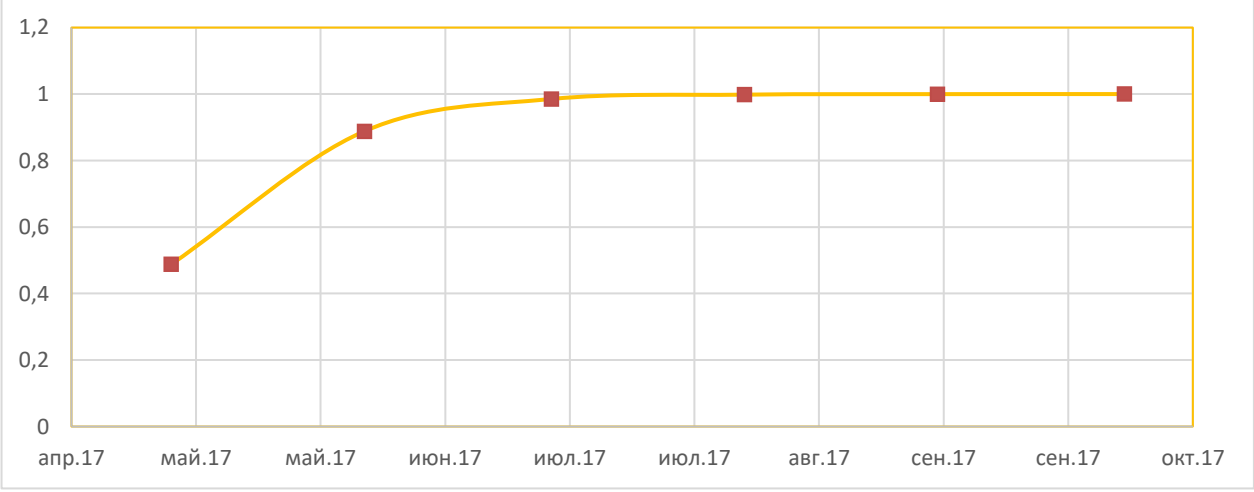

Рисунок 1. Зависимость вероятности использования ВПО *Petya* для реализации КА

Из рисунка *1* видно.

1. В июне 2017 г. $\rho_m(A) = 0{,}89$, поэтому вероятность повторения КА, аналогичной КА, реализованной с помощью ВПО *WannaCry*, был весьма высок.

2. Условная вероятность достаточности ожидаемой полезности использования КА ВПО *Petya* с точки зрения нарушителя в период с мая по сентябрь 2017 г. составила 0,99, а $P(EUA) = P(EU|A)\,P(A) \to 1$, т.е. с точки зрения нарушителя вероятность достаточности ожидаемой полезности КА вида ВПО *Petya* в мая 2017 г. оказалась близкой к 1. В связи с чем и была совершена обсуждаемая КА.

Таким образом, сравнительный анализа динамики развития КА ВПО *Petya* и результаты оценивания выбранных параметров, характеризующих данную КА, подтвердили адекватность математических моделей, описывающих процесс принятия решения нарушителем о проведении КА., а также позволили сделать следующие выводы.

1. Нецеленаправленные КА реализуются массово, как в случае с КА, в которой использовалось ВПО *Petya*. (В результате этой КА выручка нарушителя оказалась существенно выше легального заработка $W_j >> W_m$ ($W_j = 80000$, $W_m = 720000$, так как данная КА была проведена в условиях, когда был обеспечен приемлемый уровень среднего заработка от одной КА, который, с одной стороны, позволял получить ожидаемую полезность от КА, и относительно небольшую вероятность разоблачения нарушителя, с другой стороны.)

2. Успешные КА, о которых информация появляется на сайтах новостных агрегаторов, приводит к появлению «подражателей» и повторений КА. В этой связи ключевым этапом для отслеживания новых методов КА является этап Теоретической подготовки, и, в первую очередь, фаза Принятия решения, на котором отрабатывается практическая апробация метода КА.

3. Громкие уголовные дела, завершившиеся в последние 3 года наказанием нарушителей, совершающих целенаправленные КА (*http://www.tadviser.ru*), привели к существенному уменьшению средней суммы заработка нарушителя от единичной целенаправленной КА.

Разработанные математические модели были использованы далее для разработки научно обоснованной методики прогнозирования динамики вектора КА.

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. Обосновано, что единого универсального источника информации о реализованных КА сегодня не существует, поэтому в качестве источника исходных данных для определения параметров при прогнозировании вероятности КА предложено использовать данные из *DarkNet*, отчеты центров мониторинга инцидентов ИБ, а также информацию, предоставляемую новостными агрегаторами и доступную бухгалтерскую отчетность.

Разработана методика прогнозирования вектора КА, блок-схема которой представлена на рисунке 2.

Работоспособность данной методики подтверждена оценками вероятности ожидаемой полезности в 2019 г. по данным за 2017, 2018 гг. для следующего перечня перечень КА:

- 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.

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

Качественное описание прогноза векторов КА для КФС в 2019 г. определенное по разработанной методики.

1. Целевые КА на организации КФС в том виде, в котором они реализовывались в 2017 и 2018 гг. реализовываться в 2019 г. не будут, так как вероятность ожидаемой полезности при наличии возможности реализации КА данного вида равна нулю. Это означает, что группы злоумышленников будут пробовать 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 (больший рост). Это говорит о смещении фокуса 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 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 КА 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 не обладают ограничениями целевых КА с точки зрения нарушителя.

5. Увеличится вероятность реализации нецелевых КА 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).

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 КА 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 – подмена исходящего телефонного номера на номер КФС и выдача себя за сотрудника безопасности банка.

4. 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 мошеннических ресурсов в юриспруденцию иностранных доменных зон. Что говорит об изменении тренда с нецелевых КА на клиентов КФС через зараженные популярные российские сайты, на западные сайты.

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

Расчет параметров ожидаемой полезности

⇩

Оценить, используя доступные источники об успешных КА, количество выявленных КА данного типа A_m

⇩

Оценить, используя доступные источники об успешных КА, количество выявленных КА, закончившихся обращением пострадавших в правоохранительные органы и/или арестом (наказанием преступника) A_{mf}

⇩

Вычислить вероятность проведения незаметной КА

$$\rho_m = \frac{A_m - A_{mf}}{A_m}.$$

⇩

Вычислить вероятность разоблачения нарушителя

$$\rho_n = 1 - \rho_m$$

⇩

Оценить выручку нарушителя в случае успешной реализации КА W_{mp}, используя информацию о выгоде полученной нарушителем в ходе успешных реализаций аналогичных методов КА

⇩

Определить, используя общедоступные источники информации о КА, стоимость КА в сетях *DarkNet* C_j

⇩

Вычислить прибль нарушителя в случае успешной реализации КА $W_m = W_{mpj} - C_j$

⇩

Оценить текущий доход нарушителя от легальной деятельности

⇩

Определить тяжесть наказания в случае разоблачения нарушителя F_j.

⇩

Определить параметры функции

$$U(\xi) = b\ln\left(\frac{a+\xi}{a}\right),$$

⇩

Вычислить ожидаемую полезность от КА с учетом всех доходов

$$EU_{\Sigma} = (1-\rho_n)U(W_m + W_j) + \rho_n U(W_m + W_j - F_j).$$

⇩

Вычислить ожидаемую полезность от КА

$$EU_{нл} = (1-\rho_n)U(W_m) + \rho_n U(W_m - F_j).$$

⇩

Вычислить условную вероятность достаточности ожидаемой полезности

$$\rho\left(\frac{EU}{A}\right) = \frac{EU_{нл}}{EU_{\Sigma}}$$

Расчет параметров возможности реализации метода КА

⇩

Оценить, используя доступные источники об успешных КА, количество попыток реализации КА данного типа A_l

⇩

Оценить, используя доступные источники об успешных КА, количество успешно реализованных КА A_{lp}

⇩

Вычислить коэффициентом межличностной рекламы метода КА в *DarkNet*

$$a_l = \frac{A_{lp}}{A_l}.$$

⇩

Оценить, используя доступные источники об успешных КА, количество попыток апробации КА данного типа A_p

⇩

Оценить, используя доступные источники об успешных КА, количество успешно реализованных апробаций КА, определяемое на основе анализа логов центров мониторинга ИБ A_{pp}

⇩

Вычислить коэффициент апробации метода КА в *DarkNet*

$$a_p = \frac{A_{pp}}{A_p}.$$

⇩

Вычислить коэффициентом известности метода КА в *DarkNet* a_n

⇩

Вычислить параметр

$$\beta = a_n + a_l + a_p.$$

⇩

Вычислить параметр

$$\alpha_j = \frac{(1-\rho_{nj})(W_{mpj} + W_j) + \rho_{nj}(W_{mpj} + W_j - F_j)}{W_{mpj} - C_j}$$

⇩

Вычислить вероятность возможности реализации метода КА

$$p(A,t) = \frac{1}{1 + \alpha_j e^{-\beta_j t}}.$$

Рисунок 2. Методика прогнозирования вектора КА

Основные результаты работы заключаются в следующем:

1. Разработаны математические модели определения ожидаемой полезности от КА и динамики возможности реализации КА во времени с точки зрения нарушителя.
2. Проведено натурное моделирование КА, а также анализ КА ВПО *WannaCry* и *Petya*, подтверждающие полученные математические модели.
3. Разработана методика прогнозирования динамики вероятности проведения КА во времени с точки зрения нарушителя.
4. Определены источники общедоступных данных о КА для расчета параметров при прогнозировании вероятности проведения КА во времени с точки зрения нарушителя.

Перспективы дальнейшей разработки темы исследования заключаются в:

1. Определении значений параметров функции вероятности возможности реализации КА во времени на Практическом этапе и этапе Достижения цели.
2. Автоматизации сбора и анализа информации из общедоступных источников информации о КА для прогнозирования векторов КА во времени с точки зрения нарушителя.
3. Автоматизации процесса прогнозирования динамики изменения вектора КА с точки зрения нарушителя.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи, опубликованные в рецензируемых научных журналах и изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. **Макарова О.С.** 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.)
2. **Makarova O.** Computer attack`s probability function / **Makarova O.**, Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568. (0,9 п.л. / 0,45 п.л.) (Scopus)
3. **Макарова О.С.** Оценивание вероятностей компьютерных атак на основе функций / **Макарова О.С.**, Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 2. — С. 86-96. (1,1 п.л. / 0,6 п.л.)
4. **Makarova O.** 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. (0,4 п.л. / 0,2 п.л.) (Scopus)
5. **Макарова О.С.** 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. (1,3 п.л. / 0,7 п.л.)

6. **Макарова О.С.** Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» / **Макарова О.С.** // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2012. — Т. 1. № 25(2). — С. 64-68. (0,5 п.л. / 0,5 п.л.)

Другие публикации:

7. **Makarova O.** Determining the Choice of Attack Methods Approach / **Makarova Olga** // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455072 — pp. 399-402. (0,3 п.л. / 0,3 п.л.)

8. **Makarova O.** 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. (0,4 п.л. / 0,2 п.л.)

9. **Makarova O.** 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. (0,4 п.л. / 0,2 п.л.)

10. **Макарова О.С.** Моделирование непреднамеренного распространения информации пользователем / **О.С. Макарова** // Технические науки: проблемы и перспективы: материалы I Международной научной конференции (г. Санкт-Петербург, март 2011 г.). — 2011. — С. 99-103. (0,4 п.л. / 0,4 п.л.)