На правах рукописи

Бусыгин Алексей Геннадьевич

ЗАЩИТА РАСПРЕДЕЛЁННЫХ РЕЕСТРОВ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ ЦИФРОВОГО ПРОИЗВОДСТВА ОТ «АТАКИ БОЛЬШИНСТВА»

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург — 2020

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» в Институте кибербезопасности и защиты информации.

Научный руководитель:
Зегжда Дмитрий Петрович, доктор технических наук, профессор РАН, профессор

Официальные оппоненты:
Ныркov Анатолий Павлович,
доктор технических наук, профессор, профессор кафедры Комплексного обеспечения информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова».

Сухопаров Михаил Евгеньевич,
кандидат технических наук, старший научный сотрудник Лаборатории интеллектуальных систем федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации Российской академии наук.

Ведущая организация:
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Защита состоится «___» _____ г. в ___ ч. На заседании диссертационного совета У.05.13.19 на базе ФГАОУ ВО «СПбПУ» по адресу: 195251, Санкт-Петербург, ул. Политехническая, 29, ауд. 175.

С диссертацией и авторефератом можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «СПбПУ» (www.spbstu.ru).

Автореферат разослан «___» _____ г.

Ученый секретарь
диссертационного совета
У.05.13.19,
к.т.н. Лаврова Дарья Сергеевна

Общая характеристика работы

Актуальность работы. Интенсивное развитие киберфизических систем, Интернета вещей, технологий облачных вычислений и больших данных привели к появлению новой производственной парадигмы — цифровому производству. Цифровое производство основано на интегрированных друг с другом производственных системах, в режиме реального времени отвечающих изменяющимся требованиям и условиям производственных линий, логистических цепей и потребителей. В силу высокой интегрированности с критическими производственными процессами, успешная реализация угроз информационной безопасности систем цифрового производства может не только нанести финансово-экономический ущерб, но и привести к техногенным и экологическим катастрофам. Статистика роста числа атак на системы цифрового производства в совокупности с критичностью возможного ущерба, нанесённого вследствие нарушения информационной безопасности данных систем, обуславливает актуальность темы исследования. Системы распределённого реестра (СРР) являются неотъемлемой составляющей цифрового производства, обеспечивающей прозрачный информационный обмен между производственными системами. СРР, в частности, применяются для обработки информации в системах управления производственными процессами и ресурсами, цепями поставок, а также правами на цифровые объекты и модели. Общей угрозой информационной безопасности СРР является «атака большинства». Согласно статистическим данным, собранным за несколько лет, атаки данного типа значительно участились. Современные подходы и решения по защите от «атаки большинства» ограничивают масштабируемость СРР, что является критичным для систем цифрового производства. Таким образом, данное исследование, посвящённое защите СРР от «атаки большинства» в децентрализованных системах цифрового производства, является востребованным и актуальным.

Степень разработанности темы исследования. Задаче построения защищённых децентрализованных систем посвящено множество работ таких исследователей как Л. Лэмпорт, Р. Шостак, и М. Пис, Д. Долев, Г.Р. Стронг,

М. Фишер, Р. Фаулер, Н. Линч, М. Кастро и Б. Лисков, однако предложенные ими подходы обладают ограниченной масштабируемостью по количеству узлов. С. Накамото предложен подход к построению СРР, не обладающий данным ограничением. В его работе также описана «атака большинства», выполнена оценка защищённости предложенного подхода. В.М. Фомичевым и М.А. Черепневым приведены оценки защищённости СРР в случаях, когда нарушитель контролирует менее половины общей вычислительной мощности СРР. А.В. Аникиным исследованы вопросы стоимости реализации «атаки большинства» на существующие СРР. В исследовании Г. Марко-Гисберта проанализированы недостатки существующих механизмов защиты от «атаки большинства» и обозначена необходимость новых подходов к защите от данной атаки. Современные научные подходы и практические решения по защите СРР от «атаки большинства» не предлагают способов решения ряда научно-технических задач, в частности:

- оценка в реальном времени возможностей нарушителя по реализации «атаки большинства»;
- формализация признаков наличия уязвимости к «атаке большинства» для текущего состояния СРР;
- разработка методологии динамической защиты от «атаки большинства», сохраняющая возможность масштабирования СРР по количеству узлов.

Данное исследование, направленно на решение указанных выше задач.

Целью работы является защита СРР в децентрализованных системах цифрового производства от «атаки большинства», основанная на оценке вычислительных возможностей нарушителя и обеспечивающая динамическую нейтрализацию деструктивных воздействий. Для достижения поставленной цели в работе решаются следующие **задачи**:

1. Анализ особенностей СРР децентрализованных систем цифрового производства, оказывающих влияние на обеспечение защищённости от «атаки большинства».

2. Разработка подхода к оценке вычислительных возможностей нарушителя, основанного на измерении относительного падения производительности СРР.

3. Построение дискретно-событийной модели обработки транзакций в СРР децентрализованных систем цифрового производства, позволяющей в реальном времени оценивать производительность СРР.

4. Формализация показателя наличия уязвимости СРР к «атаке большинства» на основе дискретно-событийной модели обработки транзакций.

5. Разработка метода защиты СРР от «атаки большинства», основанного на динамической нейтрализации деструктивных воздействий нарушителя в период уязвимости СРР к атаке.

Научная новизна работы состоит в следующем:

1. Впервые предложен подход к осуществлению защиты от «атаки большинства», основанный на оценке вычислительных возможностей нарушителя с помощью измерения относительного падения производительности СРР.

2. Предложен показатель наличия уязвимости СРР к «атаке большинства», основанный на оценке вычислительных возможностей нарушителя в режиме реального времени.

3. Разработан метод динамической нейтрализации деструктивных воздействий нарушителя, реализующий защиту СРР в период уязвимости к «атаке большинства» путём изменения параметров обработки транзакций.

Теоретическую значимость работы составляет формализованный признак наличия уязвимости СРР к атаке большинства, позволяющий определить параметры СРР, обеспечивающие требуемый уровень защищённости от «атаки большинства».

Практическая значимость результатов работы заключается в возможности применения предложенного метода динамической защиты для обеспечения функционирования СРР в период проведения «атаки большинства» с сохранением возможности масштабирования СРР по количеству узлов.

Методы исследования. Для решения поставленных задач использовались методы математического моделирования, математической статистики и теории вероятностей, теории анализа временных рядов.

Положения, выносимые на защиту:

1. Подход к осуществлению защиты от «атаки большинства», основанный на оценке вычислительных возможностей нарушителя с помощью измерения относительного падения производительности СРР.

2. Дискретно-событийная модель обработки транзакций в СРР децентрализованных систем цифрового производств, позволяющая в реальном времени отслеживать изменения производительности СРР.

3. Формализованный показатель наличия уязвимости СРР к «атаке большинства», основанный на оценке вычислительных возможностей нарушителя.

4. Метод динамической нейтрализации деструктивных воздействий нарушителя в период уязвимости СРР к «атаке большинства».

Достоверность и обоснованность результатов, представленных в диссертации, подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Внедрение результатов работы. Подход к оценке вычислительных возможностей нарушителя, показатель наличия уязвимости СРР к «атаке большинства» и метод динамической нейтрализации деструктивных воздействий нарушителя использован в проектной деятельности АО «ЦентрИнформ» для обеспечения требуемого уровня информационной безопасности автоматизированных систем управления производственными ресурсами и процессами, а также в учебном процессе Института кибербезопасности и защиты информации ФГАОУ ВО «СПбПУ».

Апробация результатов работы. Результаты работы обсуждены на научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2016, 2017, 2018, 2019 и 2020 гг.),

научно-практической конференции «РусКрипто» (Москва, 2018, 2019 и 2020 гг.), международной конференции «Security of Information and Networks» (Кардифф, Великобритания, 2018 г.), международной научной конференции «Конвергенция цифровых и физических миров: технологические, экономические и социальные вызовы» (Санкт-Петербург, 2018 г.) и международной конференции «Региональная информатика» (Санкт-Петербург, 2016 г.).

Публикации. По теме диссертации опубликовано 14 научных работ, в том числе 4 в изданиях из перечня ВАК, 4 в изданиях, индексируемых в базах Scopus и WoS.

Объём и структура. Диссертация состоит из введения, 4 глав, заключения и списка литературы из 90 наименований.

Основное содержание работы

Во введении обоснована актуальность темы исследования, сформулированы цели и задачи работы, изложены основные результаты исследований, показана их новизна, теоретическая и практическая значимость, отражены основные положения, выносимые на защиту.

В первой главе приведены результаты анализа особенностей СРР децентрализованных систем цифрового производства, оказывающих влияние на обеспечение защищённости от «атаки большинства».

Класс СРР, использующих механизмы консенсуса, основанные на не интерактивных доказательствах проделанной вычислительной работы (proof of work), применяется в децентрализованных системах цифрового производства, поскольку обеспечивает масштабируемость СРР по количеству узлов, необходимую в силу крупномасштабности систем данного типа. Основной специфичной угрозой безопасности данного класса СРР, является «атака большинства». Данная атака направлена на нарушение целостности данных, обрабатываемых в СРР, и заключается том, что нарушитель, обладающий значительной производительностью, пытается нарушить последовательность хранящихся в СРР транзакций. Специфика атаки в системах цифрового производства заключается в необходимости получения нарушителем контроля

над узлами, обеспечивающими значительную долю производительности СРР, поскольку в силу крупномасштабности СРР собственные вычислительные возможности нарушителя не являются достаточными для реализации атаки.

Основными подходами к защите СРР от «атаки большинства» являются создание контрольных точек, введение штрафов за обработку транзакций, фиксирование транзакций проводимых в защищаемом (дочернем) СРР в дополнительном (родительском) СРР. Ограничениями данных подходов являются:

- добавление единых точек отказа единой точкой отказа;
- отсутствие защиты недавних транзакций;

– угроза атаки, заключающейся в разделении узлов СРР на две штрафующих друг друга группы;

– защита только от нарушителей, контролирующих менее половины от общей производительности СРР.

Подход, основанный на применении гибридных механизмов консенсуса, заключается в дополнении механизма консенсуса, основанного на не интерактивных доказательствах проделанной вычислительной работы, дополнительными критериями проверки и эвристиками, применяемыми в других механизмах консенсуса. Полученные в результате СРР наследуют недостатки альтернативных механизмов консенсуса, такие как ограниченная масштабируемость по числу узлов. При этом не предложено подходов к защите, основанных на динамическом комбинировании механизмов консенсуса, позволяющих обеспечить защиту от «атаки большинства» и сохранить масштабируемость СРР по количеству узлов.

Во второй главе приведены результаты формализации показателя наличия уязвимости СРР к «атаке большинства» на основе дискретно-событийной модели обработки транзакций. Для формализации показателя наличия уязвимости были разработаны:

- подход к оценке вычислительных возможностей нарушителя, основанного на измерении относительного падения производительности СРР;

- дискретно-событийной модели обработки транзакций, позволяющая в реальном времени отслеживать изменения производительности СРР.

Предложенный подход к оценке вычислительных возможностей нарушителя (производительности узлов СРР, контролируемых нарушителем), заключается в следующем. Пусть $\mathbb{V}$ — множество узлов СРР. Каждый узел $v \in \mathbb{V}$ характеризуется производительностью $h(v)$ — числом операций поиска решения задачи создания нового блока (взятия хэш-образа от блока транзакций), выполняемых за единицу времени. Рассмотрим процесс обработки транзакций, осуществляемый узлами СРР на временном интервале Δt. Пусть $\boldsymbol{r}(v)$ — множество возможных решений задачи создания нового блока транзакций, проверяемых узлом $v \in \mathbb{V}$ за время Δt, т.е. $\#\boldsymbol{r}(v) = h(v)\Delta t$. При этом множества проверяемых узлами решений формируется так, чтобы выполнялось условие (1):

$$\forall v', v'' \in \mathbb{V}: \#\big(\boldsymbol{r}(v') \cap \boldsymbol{r}(v'')\big) \approx 0. \quad (1)$$

Тогда производительность СРР H_0 можно оценить с помощью (2):

$$H_0 \approx \sum_{v \in \mathbb{V}} h(v). \quad (2)$$

Положим, что множество $\mathbb{V}$ фиксировано, тогда для реализации «атаки большинства» нарушителю необходимо переключить узлы из контролируемого им подмножества $\mathbb{V}_A \subseteq \mathbb{V}$, $\mathbb{V}_A \neq \emptyset$ с генерации основной цепочки блоков, на генерацию альтернативной цепочки блоков. Тогда производительность СРР после начала атаки H_A можно оценить с помощью (3):

$$H_A \approx \sum_{v \in \mathbb{V} \setminus \mathbb{V}_A} h(v). \quad (3)$$

Так как $H_0 > H_A$, произойдёт падение производительности СРР. Таким образом производительность узлов, контролируемых нарушителем, можно оценить как ΔH (4):

$$\Delta H = H_0 - H_A. \quad (4)$$

Для оценки текущей производительности СРР разработана следующая дискретно-событийную модель обработки транзакций.

$\mathbb{T}$ — часы, синхронизирующие возникновение событий. Каждому событию в рамках данной модели сопоставляется временная метка $t \in \mathbb{T}$.

$\mathbb{X} \neq \emptyset$ — множество транзакций, обрабатываемых СРР.

$\mathbb{Q}$ — множество конечных последовательностей транзакций из $\mathbb{X}$.

В предложенной дискретно-событийной модели состояние СРР определяется парой $S = \langle B, Q \rangle$, где:

$Q \in \mathbb{Q}$ — конечная последовательность необработанных транзакций;

B — конечная последовательность блоков транзакций (4):

$$B = \{\langle b_i, t_i \rangle\}_{i=0}^{L_B}, L_B > 0,$$
$$b_i \in \mathbb{H} \times \mathbb{N} \times \mathbb{Q}, \quad (4)$$
$$t_i \in \mathbb{T}, t_{i-1} < t_i,$$

где $\mathbb{H} = \{0, 1, 2, \dots, 2^n - 1\}$ — множество значений n-разрядной криптографической хэш-функции $\mathcal{H}$;

$\mathbb{N}$ — множество натуральных чисел, включающее 0.

Значение $\mathcal{H}_{\max} \in \mathbb{H}$ задаёт сложность задачи создания нового блока.

Состояние СРР в начальный момент времени определено следующим образом (5):

$$S = \langle B = \{\langle b_0, t_0 \rangle\}, Q = \emptyset \rangle, \qquad b_0 = \langle 0, 0, \emptyset \rangle. \quad (5)$$

В рамках модели определены следующие события:

1) Появление транзакции $x \in \mathbb{X}$. Обработка данного события заключается в добавлении x в конец последовательности Q. В рамках данной модели все появляющиеся транзакции полагаются корректными и не противоречащими S.

2) Появление возможного решения задачи создания нового блока $r \in \mathbb{N}$. События данного типа возникают с частотой H равной производительности СРР. Обработка события в данной модели заключается в проверке условия (6) для $b = \langle \mathcal{H}(b_{L_B}), r, Q \rangle$:

$$\mathcal{H}(b) \leq \mathcal{H}_{\max}. \quad (6)$$

Если условие выполняется, то в конец B добавляется новый элемент $\langle b, t \rangle$, где t — временная метка события, а также $Q \leftarrow \emptyset$.

3) Появление альтернативной последовательности блоков транзакций $B' = \{\langle b'_i, t'_i \rangle\}_{i=0}^{L_{B'}}$. Для B' проверяется выполнение условий (7):

$$\begin{gathered}(b'_0 = \langle 0, 0, \emptyset \rangle) \wedge (t'_0 = t_0), \\ \forall \langle b'_i, t'_i \rangle \in B' : (t'_i > t'_{i-1}) \wedge (\mathcal{H}(b'_i) \leq \mathcal{H}_{\max}) \wedge (L_{B'} > L_B).\end{gathered} \tag{7}$$

Если условия выполняются, то $B \leftarrow B'$, $Q \leftarrow \emptyset$.

Предложенная модель позволяет оценить производительность СРР, используя только значение B. Положим, что значения $\mathcal{H}$ распределены равномерно, тогда число попыток нахождения такого r, для которого выполняется (6), случайной величиной с геометрическим распределением. Её математическое ожидание равно (8):

$$M = \frac{2^n}{\mathcal{H}_{\max} + 1}. \tag{8}$$

Таким образом, производительность СРР H_i в момент генерации блока транзакций $\langle b_i, t_i \rangle$ может быть оценена с помощью среднего значения для k последних блоков (9):

$$H_i(k) = \frac{Mk}{t_i - t_{i-k}}, \qquad k > 0. \tag{9}$$

Уязвимость распределённого реестра к «атаке большинства» можно определить через вероятность P успешной реализации данной атаки. В работе С. Накамото была дана следующая оценка вероятности успешной реализации «атаки большинства» (10):

$$P = \begin{cases} 1 - \sum_{i=0}^{z} \frac{\lambda^i e^{-\lambda}}{i!} \left(1 - \left(\frac{q}{1-q}\right)^{z-i}\right), & q < \frac{1}{2}, \\ 1, & q \geq \frac{1}{2}. \end{cases} \tag{10}$$

где $\lambda = z\frac{q}{q-1}$;

q — вероятность того, что следующий блок транзакций в последовательности B будет сгенерирован узлами, контролируемыми нарушителем;

z — минимальное количество подтверждающих блоков, которое должно следовать за блоком с транзакцией для того, чтобы транзакция считалась выполненной. Значение z является константным параметром, заданным для СРР.

Задача применения (10) для оценки вероятности успешной реализации «атаки большинства» для состояния текущего состояния S СРР осложняется тем, что значение параметра q в произвольный момент времени не известно. Предложенный подход и дискретно-событийная модель позволяют выполнить оценку q с помощью (11):

$$q_i = \frac{\Delta H + H'_A}{H_0}, \qquad (11)$$
$$H_0 = H_{i-k''}(k'), \qquad \Delta H = H_0 - H_i(k''), \qquad k' > k'',$$

где i — номер блока транзакций, для которого выполняется оценка, H'_A — производительность узлов нарушителя, не задействованных в обработке транзакций СРР до начала «атаки большинства». Значение H'_A может быть оценено на основе модели нарушителя и пренебрежимо мало для крупномасштабных СРР.

На основе оценки вероятности успешной реализации атаки предложен следующий показатель наличия уязвимости СРР к «атаке большинства». СРР уязвима к «атаке большинства» на момент времени генерации i-ого блока, если вероятность успешной реализации атаки превышает заданное пороговое значение P_{max} (12):

$$vuln(i) = \begin{cases} 1, & P_i > P_{max} \\ 0, & P_i \le P_{max} \end{cases},$$

$$P_i = \begin{cases} 1 - \sum_{j=0}^{z} \frac{\lambda_i^j e^{-\lambda_i}}{j!} \left(1 - \left(\frac{q_i}{1-q_i}\right)^{z-j}\right), & q_i < \frac{1}{2}, \\ 1, & q_i \ge \frac{1}{2}, \end{cases} \qquad (12)$$

$$\lambda_i = z\frac{q_i}{1-q_i}.$$

В качестве порогового значения P_{max} выбирается максимальное значение вероятности успешной «атаки большинства», которое допустимо для защищаемой

СРР. Конкретное значение выбирается по результатам оценки рисков и зависит от критичности обрабатываемых в СРР данных.

Для данного показателя получены следующие оценки вероятности ошибок первого (13) и второго (14) рода:

$$P_I = 1 - \sum_{i=k''}^{m} \left(C_{i-1}^{k''-1} \left(1 - \frac{1}{M}\right)^{i-k''} \left(\frac{1}{M}\right)^{k''} \right), \qquad m = \left\lfloor \frac{k''M}{1-\hat{q}} \right\rfloor. \tag{13}$$

$$P_{II} = \sum_{i=k''}^{m} \left(C_{i-1}^{k''-1} \left(1 - \frac{1}{M}\right)^{i-k''} \left(\frac{1}{M}\right)^{k''} \right), \qquad m = \left\lfloor \frac{k''H_A M}{(1-\hat{q})H_0} \right\rfloor, \tag{14}$$

где $\hat{q}$ — значение параметра q, при котором вероятность успешной атаки равна P_{max}, H_A — реальная производительность СРР во время атаки.

В третьей главе приведён разработанный метод динамической нейтрализации деструктивных воздействий нарушителя, реализующей защиту СРР в период уязвимости к «атаке большинства» путём изменения параметров обработки транзакций

Предложенный показатель позволяет наличия уязвимости для текущего состояния СРР. При переходе СРР в уязвимое состояние требуется выполнить действия по нейтрализации деструктивных воздействий нарушителя. В качестве решения данной задачи предлагается осуществлять динамическое переключение СРР на использование механизма консенсуса, основанного на голосовании. Функции обработки транзакций делегируются подмножеству узлов СРР. Предполагается, что подмножество голосующих узлов состоит из доверенных узлов.

Переход на использование механизма консенсуса, основанного на голосовании, осуществляется при выполнении условия (15):

$$\sum_{j=0}^{z} vuln(L_B - j) > u\,, \qquad u \le z. \tag{15}$$

Параметры u выбирается таким образом, чтобы получить необходимое соотношение вероятностей ошибок первого рода $P_I^{(м)}$ (16) и второго рода $P_{II}^{(м)}$ (17):

$$P_I^{(\text{м})} = \sum_{i=s}^{r} C_r^i (1 - P_I)^{r-i} P_I^i, \qquad r = z - k + 1, s = u. \tag{16}$$

$$P_{II}^{(\text{м})} = \sum_{i=s}^{r} C_r^i (1 - P_{II})^{r-i} P_{II}^i, \qquad r = z - k + 1, s = r - u + 1. \tag{17}$$

Возврат к использованию механизма консенсуса, основанного на доказательстве выполненной работы, происходит при возвращении производительности СРР к исходному значению для не менее чем z генерируемых подряд блоков.

Данный метод защиты нейтрализует возможности нарушителя по проведению «атаки большинства», а также компенсирует падение производительности СРР, наблюдаемое в начале атаки. Разработанный метод сохраняет возможность масштабирования СРР по количеству узлов, поскольку переключение на механизм консенсуса, основанный на голосовании, выполняется лишь на период времени, в течение которого СРР уязвим к «атаке большинства».

В четвёртой главе описываются результаты экспериментальных исследований, подтверждающие корректность предложенного метода.

С целью подтверждения корректности предложенного метода защиты СРР от «атаки большинства» было выполнено моделирование СРР с различными параметрами общей производительности, числом подтверждающих блоков, производительности узлов, контролируемых нарушителем. Получены значения

Например, для параметров $k' = 20$, $k'' = 5$, $u = 3$, $P_{max} = 0{,}1$ и 1000 испытаний были получены значения точности выявления уязвимых состояний СРР, приведённые в таблице 1.

Таблица 1 — Точность выявления уязвимых состояний СРР

Ошибки	**Теоретическая оценка вероятности ошибки**	**Доля ошибок полученная экспериментально**
Ошибки первого рода	0,077	0,081
Ошибки второго рода	0,077	0,073

На рисунке 3 приведён пример обнаружения уязвимого состояния СРР для одного из экспериментов.

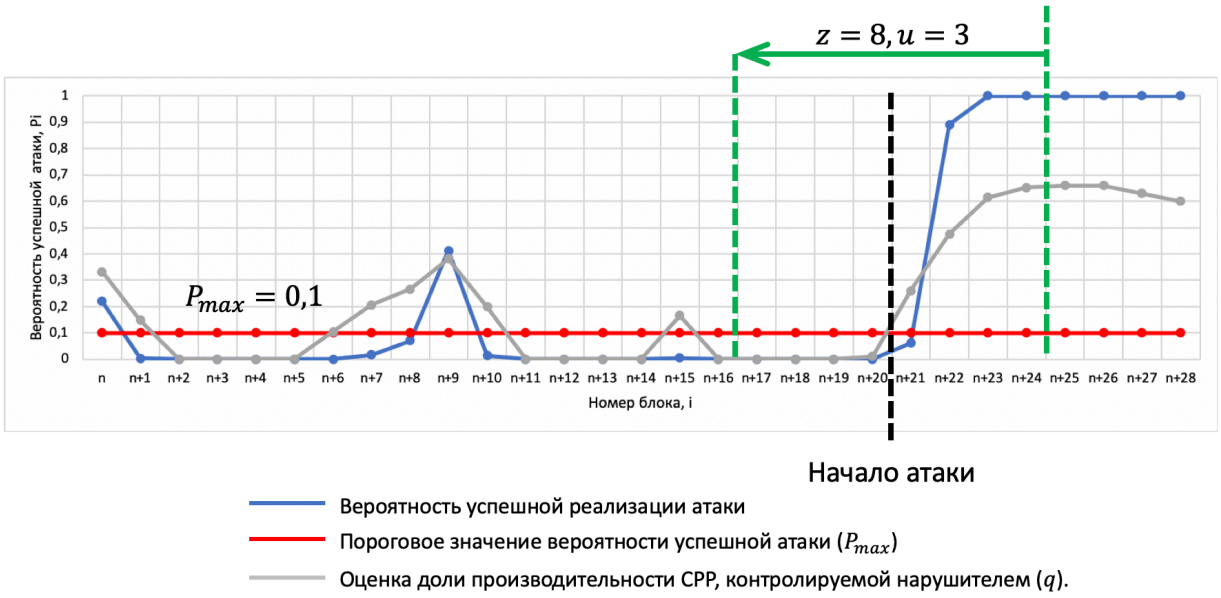

Рисунок 3 — Обнаружение уязвимого состояния СРР

Атака начинается после создания блока с номером $n + 20$. На рисунке видно, что уязвимое состояние обнаруживается после генерации 4 блоков транзакций с момента начала атаки. Уязвимое состояние обнаруживается успешно, т.е. до момента генерации последнего подтверждающего блока $n + 28$.

Полученные экспериментальные результаты подтверждают применимость предложенного метода для защиты СРР от «атаки большинства», демонстрируя успешное выявление уязвимых состояний СРР.

В заключении приведены основные результаты и выводы, полученные в ходе выполнения работы.

Основные результаты работы

В результате диссертационного исследования предложен и реализован подход к обеспечению защиты СРР в децентрализованных системах цифрового производства от «атаки большинства», основанный на оценке вычислительных возможностей нарушителя и обеспечивающий динамическую нейтрализацию деструктивных воздействий. Получены следующие результаты:

1. Выполнен анализ особенностей СРР децентрализованных систем цифрового производства и определена специфика, и позволяющая оценить вычислительные возможности нарушителя. Данная специфика заключается в необходимости получения нарушителем контроля над узлами, обеспечивающими значительную долю производительности СРР, поскольку в силу крупномасштабности СРР собственные вычислительные возможности нарушителя не являются достаточными для реализации атаки. Выявлены и преодолены ограничения существующих подходов к защите СРР от «атаки большинства».

2. Впервые предложен подход к оценке вычислительных возможностей нарушителя на основе измерения относительного падения производительности СРР.

3. Построена дискретно-событийная модель обработки транзакций в СРР децентрализованных систем цифрового производств, позволяющая в реальном времени отслеживать изменения производительности СРР, на основе моделирования числа операций, необходимых для обработки новых транзакций, с помощью случайной величины с геометрическим распределением.

4. Формализован показатель наличия уязвимости СРР к «атаке большинства», на основанный на оценке вычислительных возможностей нарушителя, позволяющий реализовать динамическую защиту СРР от данной атаки, а также определить параметры СРР, обеспечивающие требуемый уровень защищённости.

5. Разработан метод защиты СРР от «атаки большинства», основанный на динамической нейтрализации деструктивных воздействий нарушителя в период уязвимости СРР путём изменения параметров обработки транзакций. Разработанный метод сохраняет возможность масштабирования СРР по количеству узлов.

Основные результаты диссертационной работы изложены в 14 публикациях.

Публикации в изданиях, из перечня ВАК РФ:

1. Бусыгин, А.Г. Модель основанной на технологии блокчейн системы для оценки защищенности от угроз, обусловленных неравномерным распределением вычислительных мощностей / А.Г. Бусыгин // Проблемы информационной безопасности. Компьютерные системы. — 2019. — №4. — С. 114-117.

2. Бусыгин, А.Г. Обеспечение устойчивости функционирования саморегулирующейся киберфизической системы при помощи методов адаптивного управления топологией с применением блокчейн-подобного ориентированного ациклического графа / А.Г. Бусыгин, А.С. Коноплев, Д.П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. — 2018. — №2. — С. 137-140.

3. Бусыгин, А.Г. Метод сокращения объёма данных в блокчейн-подобном ориентированном ациклическом графе, применяемом для защиты данных в высоконагруженных системах / А.Г. Бусыгин, А.С. Коноплев, Д.П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. — 2018. — №2. — С. 131-136.

4. Коноплев, А.С. Модель децентрализованной инфраструктуры открытых ключей на основе технологии Блокчейн / А.С. Коноплев, А.Г. Бусыгин, Д.П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. — 2017. — №3. — С. 91-97.

Публикации в изданиях, индексируемых Scopus и WoS:

5. Busygin, A.G. Providing Stable Operation of Self-Organizing Cyber-Physical System via Adaptive Topology Management Methods Using Blockchain-Like Directed Acyclic Graph / A.G. Busygin, A.S. Konoplev, D.P. Zegzhda // Automatic Control and Computer Sciences. — 2018. — Vol. 52. — No. 8. — Pp. 1080-1083. (Бусыгин, А.Г. Обеспечение устойчивости функционирования саморегулирующейся киберфизической системы при помощи методов адаптивного управления топологией с применением блокчейн-подобного ориентированного ациклического графа / А.Г. Бусыгин, А.С. Коноплев, Д.П. Зегжда // Automatic Control and Computer Sciences. — 2018. — Т. 52. — №8. — С. 1080-1083.)

6. Konoplev, A.S. A Blockchain Decentralized Public Key Infrastructure Model / A.S. Konoplev, A.G. Busygin, D.P. Zegzhda // Automatic Control and Computer Sciences. — 2018. — Vol. 52. — No. 8. — Pp. 1017-1021. (Коноплев, А.С. Модель децентрализованной инфраструктуры открытых ключей на основе технологии Блокчейн / А.С. Коноплев, А.Г. Бусыгин, Д.П. Зегжда // Automatic Control and Computer Sciences. — 2018. — Т. 52. — №8. — С. 1017-1021.)

7. Busygin, A. Floating Genesis Block Enhancement for Blockchain Based Routing Between Connected Vehicles and Software-defined VANET Security Services / A. Busygin, A. Konoplev, M. Kalinin, D. Zegzhda // In Proceedings of 11th International Conference on Security of Information and Networks (SIN'18), Cardiff; United Kingdom; September 10-12, 2018. — ACM New York, USA. — Article No. 24. (Бусыгин, А. Улучшение основанной на технологии Блокчейн маршрутизации между транспортной сетью и программно-конфигурируемыми сервисами безопасности VANET с помощью метода плавающего генезис-блока / А. Бусыгин, А. Коноплев, М. Калинин, Д. Зегжда // В сборнике материалов 11 международной конференции по безопасности информации и сетей, Кардифф; Соединённое Королевство; сентябрь 10-12, 2018. — ACM Нью-Йорк, США. — Статья №24.)

8. Busygin, A. Supporting connectivity of VANET/MANET network nodes and elastic software-configurable security services using blockchain with floating genesis block / A. Busygin, M. Kalinin, A. Konoplev // SHS Web of Conferences 44 00020 (2018), IV International Scientific Conference "The Convergence of Digital and Physical Worlds: Technological, Economic and Social Challenges" (CC-TESC2018). (Бусыгин, А. Поддержание связности между узлами сетей VANET/MANET и эластичными программно конфигурируемыми сервисами безопасности с посощью блокчейна с плавающим генезис-блоком / А. Бусыгин, М. Калинин, А. Коноплев // SHS Web of Conferences 44 00020 (2018), IV международная научная конференция «Конвергенция цифровых и физических миров: технологические, экономические и социальные вызовы» (CC-TESC2018).)

В других изданиях:

9. Бусыгин, А.Г. Метод защиты распределённых реестров от «атаки большинства» / А.Г. Бусыгин // Сб. материалов 29 научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — СПб.: Изд-во Политехн. ун-та., 2020. — С. 4-5.

10. Бусыгин, А.Г. Обнаружение скомпрометированных узлов динамических сетей интернета вещей при помощи децентрализованных моделей доверия с применением технологии блокчейн / А.Г. Бусыгин // Сб. материалов 28 научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — СПб.: Изд-во Политехн. ун-та., 2019. — С. 75-76.

11. Бусыгин, А.Г. Архитектура устойчивой саморегулирующейся киберфизической системы / А.Г. Бусыгин, А.С. Коноплев // Сб. материалов 27 научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — СПб.: Изд-во Политехн. ун-та., 2018. — С. 95-97.

12. Бусыгин, А.Г. Применение технологии Блокчейн для поддержания связности узлов в самоорганизующихся сетях / А.Г. Бусыгин, А.С. Коноплев // Сб. материалов 26 научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — СПб.: Изд-во Политехн. ун-та., 2017. — С. 101-102.

13. Бусыгин, А.Г. Применение технологии Блокчейн для управления доступом в децентрализованных системах / А.Г. Бусыгин, А.С. Коноплев // Сб. материалов XV Санкт-Петербургской международной конференции «Региональная информатика (РИ-2016)». — СПб.: Изд-во СПИИРАН, 2016. — С.325.

14. Коноплев, А.С. Применение технологии блокчейн для построения децентрализованной инфраструктуры открытых ключей / А.С. Коноплев, А.Г. Бусыгин // Сб. материалов 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». — СПб.: Изд-во Политехн. ун-та., 2016. — С.17-18.