УДК 004.056

ГИБКАЯ СИСТЕМА УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ ЦИФРОВЫХ ПЛАТФОРМ ЭКОНОМИКИ НА БАЗЕ ТЕХНОЛОГИИ ПКС

В.М. Крундышев
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: vmk@ibks.spbstu.ru

П.Д. Зегжда
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: zeg@ibks.spbstu.ru

М.О. Калинин
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: max@ibks.spbstu.ru

Ключевые слова: информационная безопасность, программно-конфигурируемые сети, управление кибербезопасностью, цифровая экономика, ПКС.

Аннотация: Переход от информационной экономики к цифровой ставит перед обществом новые вызовы, связанные с развитием прорывных технологий: интернет вещей, сети киберфизических систем, искусственный интеллект, большие данные. При создании цифровых платформ возникает ряд трудностей: большая размерность цифровой инфраструктуры и ее неоднородность, плохо налаженное информационное взаимодействие между сегментами, отсутствие единого подхода к обеспечению кибербезопасности и высокая зависимость от квалификации персонала и надежности оборудования. Внедрение цифровой экономики ведет к повышению риска киберугроз, связанных с проблемами управления доступом между системами, регулирования информационных и управляющих потоков. В статье предлагается программно-конфигурируемый подход к обеспечению автоматического управления кибербезопасностью цифровых платформ экономики, разработаны архитектуры системы ПКС-управления, а также проведена сравнительная оценка их эффективности.

1. Введение

Цифровая трансформация и интернетизация экономики являются драйвером современного подхода к обеспечению кибербезопасности. В традиционных компьютерных сетях объектом защиты являлась совокупность данных ограниченного доступа, а задача защиты информации заключалась в обеспечении конфиденциальности, целостности и доступности [1]. В последнее десятилетие в связи с активным развитием динамических межмашинных цифровых инфраструктур (например, IoT [2], IIoT [3], WSN [4], MANET [5], VANET [6]) объект защиты приобретает новое представление как эле-

мент киберсреды, где традиционные операции чтения/записи имеют физические последствия, при этом основной задачей стало обеспечение сохранности и надежности киберсистем, а также, как следствие, жизни людей. Из-за особенностей современных цифровых инфраструктур и стремительно растущего объема данных, подвергающихся обработке, традиционные методы защиты становятся неэффективными, поэтому перед исследователями стоит задача создания новых методов обеспечения кибербезопасности, которые отвечают актуальным вызовам времени – методов управления доступом между системами в динамической инфраструктуре, глобального регулирования информационных и управляющих потоков.

Авторами предлагается программно-конфигурируемый подход к обеспечению автоматического управления кибербезопасностью цифровых платформ экономики, разработаны архитектуры системы ПКС-управления, а также проведена сравнительная оценка их эффективности.

2. Подход на базе технологии программно-конфигурируемых сетей

В качестве основы для решения обозначенной проблемы предлагается использовать технологию программно-конфигурируемых сетей (ПКС, software-defined networks, SDN). ПКС представляет собой интеллектуальную систему управления, которая напрямую взаимодействует со средой передачи данных. ПКС являются более гибкими, по сравнению с традиционными сетями, структурами и позволяют динамически вносить изменения в правила маршрутизации в соответствии с задачами, которые должна решать сеть [7], включая задачи безопасности. Центром управления в такой сети выступает выделенный сервер с программным ПКС-контроллером.

ПКС позволяет реализовать принцип программно-конфигурируемой безопасности (ПКБ, SDS – software-defined security) – технологии управления безопасностью всей сети в целом с помощью программных сетевых сервисов управления, выполняющихся на ПКС-контроллере (управления маршрутизацией, мониторингом, контролем доступа и пр.), подключенном по протоколу OpenFlow к узлам системы [8].

Предложены три варианта архитектуры внедрения механизмов кибербезопасности в цифровые платформы экономики, которые разработаны на основе технологии ПКС:

- архитектура с центральным звеном управления – серверами, решающими задачи безопасности (рис. 1);
- архитектура с частичной децентрализацией (рис. 2);
- иерархическая архитектура (рис. 3).

Для сопоставления разработанных архитектур выполнено экспериментальное исследование. В качестве критериев оценки выбраны технические параметры: пропускная способность, доля доставленных пакетов, временная задержка, среднее время обнаружения атак типов «Черная дыра», «Червоточина», «Отказ в обслуживании» (как примеры специфических кибератак на гибкие динамически изменяемые инфраструктуры [9]). Для проведения экспериментов использован эмулятор – Mininet-WiFi [10]. Размер экспериментальной сети 100 узлов, вариативность топологии системы – 0…20 м/с. Расположение узлов в заданной области происходит случайном образом, среднее расстояние между узлами составляет 50 м. Результаты приведены в таблице 1.

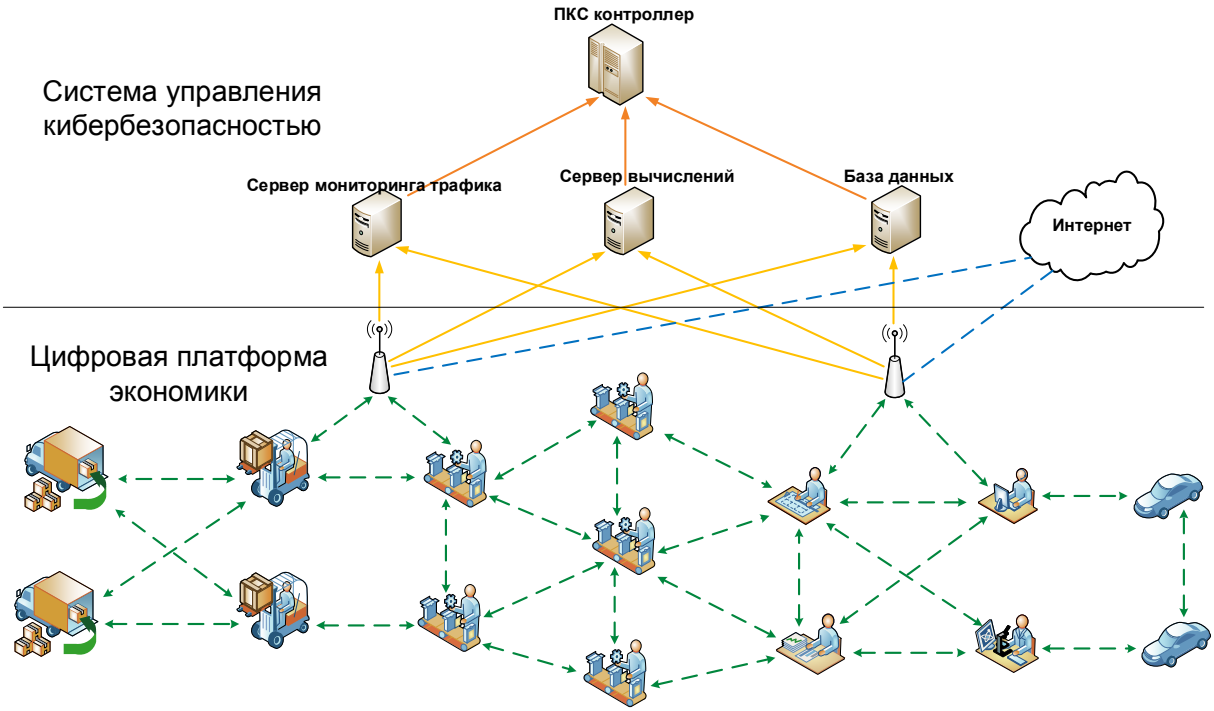

Рис. 1. Архитектура ПКС-системы управления кибербезопасностью цифровых платформ с центральным звеном.

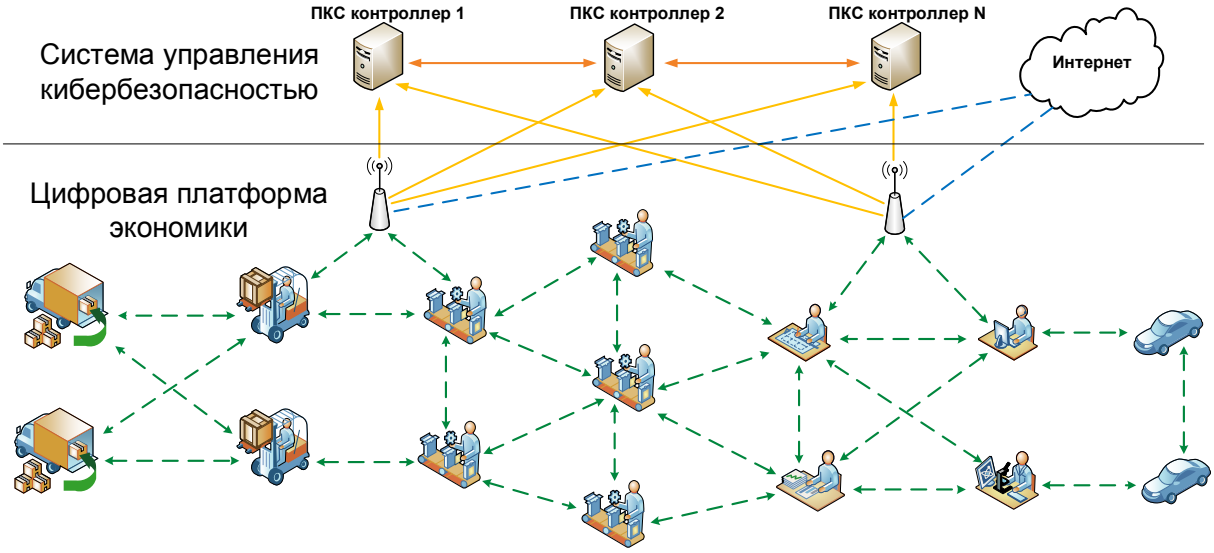

Рис. 2. Архитектура ПКС-системы управления кибербезопасностью цифровых платформ с частичной децентрализацией.

В результате проведенных экспериментов можно сделать вывод, что применение технологии ПКС позволяет решить существующие проблемы безопасности цифровых платформ, а именно: проблему обеспечения помехоустойчивости, проблему обеспечения безопасности передаваемых данных на уровне контроля доступа и изоляции потоков, проблему общей пропускной способности и проблему динамической топологии. Наилучшие тактико-технические характеристики управления обеспечиваются при использовании иерархической ПКС-архитектуры.

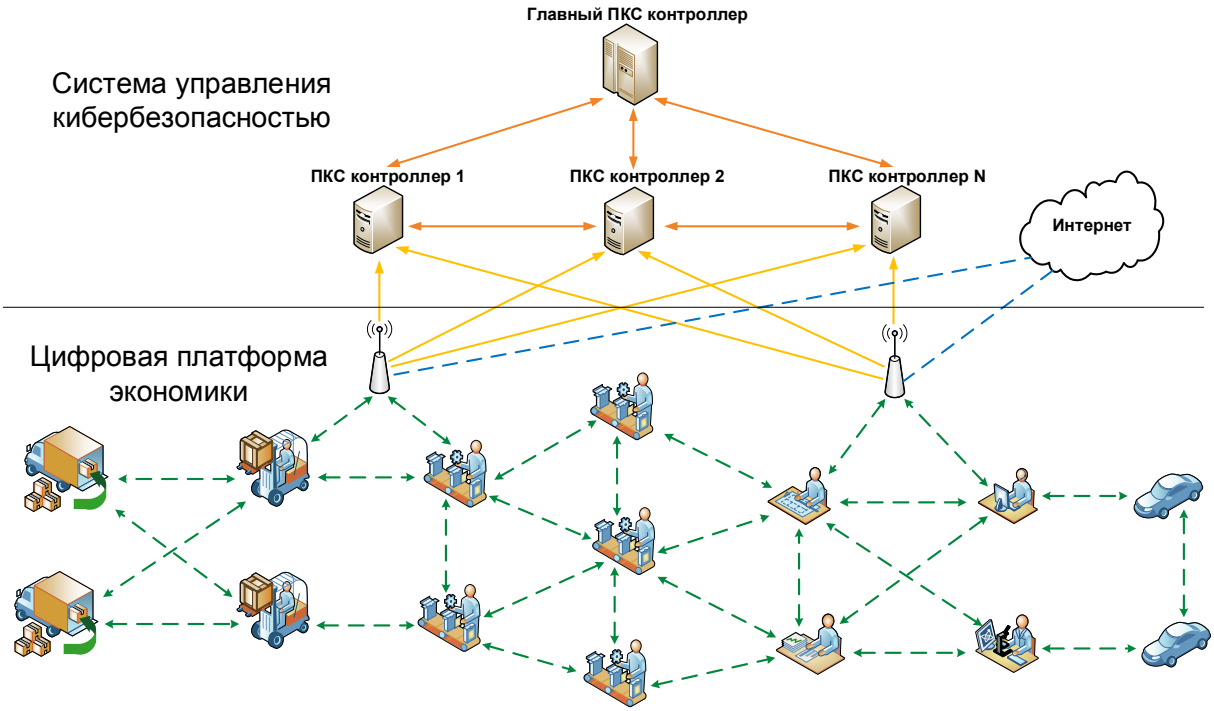

Рис. 3. Иерархическая архитектура ПКС-системы управления кибербезопасностью цифровых платформ.

Таблица 1. Сравнение эффективности разработанных архитектур системы управления кибербезопасностью цифровых платформ.

	Централизованная архитектура	**Архитектура с частичной децентрализацией**	**Иерархическая архитектура**
Пропускная способность, Кбит/с	780	820	970
Доля доставленных пакетов, %	88	92	99
Средняя временная задержка, мс	70	70	40
Время обнаружения кибератак, мс	860…990	720…910	600…730

3. Заключение

Использование технологии ПКС при построении цифровых платформ экономики позволяет повысить их уровень кибербезопасности. Предложенный подход позволяет установить политику безопасности в контролируемой системе, увеличить пропускную и мобилизационную способность платформы, уменьшить время реакции системы на внешние воздействия. На главном ПКС-контроллере иерархической системы управления возможен сбор и обработка больших данных о состоянии всей системы. За счет этого повышаются удобство управления, безопасность системы и упрощается выполнение ряда сервисных задач: реализуется мониторинг и разделение потоков данных и управления, ситуационное реагирование на инциденты, управление приоритетами по типам взаимодействия, автоматизация реагирования инфраструктуры при нападениях, межузловых заторах и сбоях оборудования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №18-29-03102.

Результаты работы получены с использованием вычислительных ресурсов суперкомпьютерного центра Санкт-Петербургского политехнического университета Петра Великого – СКЦ «Политехнический» (http://www.spbstu.ru).

Список литературы

1. Зегжда Д.П., Ивашко А.М. Основы информационной безопасности информационных систем // Горячая линия – Телеком. 2000.
2. Lavrova D., Pechenkin A., Gluhov V. Applying correlation analysis methods to control flow violation detection in the internet of things // Automatic Control and Computer Sciences. 2015. Vol. 49, No. 8. P. 735-740.
3. Sisinni E. et al. Industrial Internet of Things: Challenges, Opportunities, and Directions // IEEE Transactions on Industrial Informatics, 2018. Vol. 14. No. 11. P. 4724-4734.
4. Овасапян Т.Д., Иванов Д.В., Зегжда Д.П. Обеспечение безопасности wsn-сетей на основе модели доверия // Региональная информатика и информационная безопасность. 2017. С. 421-422.
5. Singh R., Nand P. Literature review of routing attacks in MANET // 2016 International Conference on Computing, Communication and Automation (ICCCA). Noida, 2016. P. 525-530.
6. Belenko V., Krundyshev V., Kalinin M. Synthetic datasets generation for intrusion detection in VANET // Proceedings of the 11th International Conference on Security of Information and Networks. 2018.
7. Крундышев В.М., Калинин М.О., Зегжда Д.П. Моделирование и исследование свойств безопасности перемещающихся программно-конфигурируемых сетей VANET/MANET с использованием виртуальной среды суперкомпьютера // Информационная безопасность регионов России (ИБРР-2017). Санкт-Петербург, 1-3 ноября 2017 г. С. 280-282.
8. El Moussaid N., Toumanari A., El Azhari M. Security analysis as software-defined security for SDN environment // 2017 Fourth International Conference on Software Defined Systems (SDS). Valencia, 2017. P. 87-92.
9. Калинин М.О., Крундышев В.М., Семьянов П.В. Архитектуры построения защищенных транспортных сетей на основе технологии SDN // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 53-61.
10. Mininet-WiFi. https://github.com/intrig-unicamp/mininet-wifi/