REDS:

Телекоммуникационные устройства и системы

№3

2023

СОДЕРЖАНИЕ

ИСПОЛЬЗОВАНИЕ ГИБРИДНЫХ СЕТЕЙ СПУТНИКОВОГО ДОСТУПА В СИСТЕМАХ ИНДИВИДУАЛИЗИРОВАННОГО СПАСЕНИЯ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Босомыкин Дмитрий Васильевич,
ФГУП НИИР, директор НТЦ. Москва, Россия

Сарьян Вильям Карпович,
ФГУП НИИР, академик НАН РА, профессор, д.т.н., Москва, Россия
sarian@niir.ru

Парамонов Александр Иванович,
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», д.т.н, Санкт-Петербург, Россия
alex-in-spb@yandex.ru

Викулов Антон Сергеевич,
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», к.т.н., Санкт-Петербург, Россия

Аннотация
В условиях чрезвычайных ситуаций, таких как техногенные и природные катастрофы, задача обеспечения спасения людей является наиболее приоритетной. Вместе с тем, в таких условиях надежность и даже работоспособность систем стационарной связи может быть под вопросом. Поэтому обеспечение системы индивидуализированного управления спасением людей должно включать в себя задействование всех возможных средств связи с целью донести персонально до конкретного человека (пользователя) необходимой информации. В этом ключе перспективным видится интеграция систем мобильной связи пятого и последующих поколений с системами спутникового доступа с созданием гибридной сети. В данной работе рассмотрены основные преимущества такого подхода.

Ключевые слова: *Беспроводная сеть доступа, гибридная сеть, спутниковая сеть доступа, индивидуализированное управление спасением*

Введение

Система индивидуализированного управления спасением абонентов (ИУСА) в настоящее время рассматривается как одно из перспективных средств, позволяющих повысить для человека шансы на спасение в условиях возникновения и развития опасной для жизни чрезвычайной ситуации (ЧС).

В ее рамках основной задачей системы связи является обеспечение возможности информационного взаимодействия с людьми, оказавшимися в зоне ЧС. Обеспечение такого взаимодействия является важнейшей задачей, решение которой можно отнести к организационной междисциплинарной системе [1].

Современное развитие цифровых технологий, играет все большую роль в предоставлении массовых инфокоммуникационных (ИК) услуг, в том числе и услуг управления. ИУСА – это предоставление ИК услуг управления человеку может быть основной целью функционирования и управления в современной междисциплинарной среде [2].

В исследованиях отмечалось, что ИУСА может быть применена в том числе и с задействованием существующих инфраструктур БЛВС [3]. Так, высокая плотность точек доступа WLAN в существующей городской инфраструктуре потенциально может существенно повысить доступность услуг связи [2]. Здесь необходимо отметить все большее внедрение технологий “4G offload”, позволяющих переносить часть нагрузки с сотовых сетей мобильной связи на стационарные БЛВС. Таким образом достигнутое повышение доступности услуг связи является как положительным результатом для развития инфокоммуникационной системы в целом, так и весьма значимым фактором повышения устойчивости функционирования системы связи в условиях воздействия деструктивных и опасных для человека факторов, например, в условиях ЧС, вызванных самыми различными причинами.

В условиях ЧС, как правило, резко возрастает трафик пользователей в сети общего доступа [4], что вызвано нехваткой информации и необходимостью привлечения помощи. Этот процесс с высокой вероятностью может привести к обратному эффекту, т.е. перегрузкам сети и снижению доступности информации.

Для повышения эффективности мер по спасению людей в условиях ЧС важнейшую роль играет рациональная организация действий, оказавшихся в опасной зоне людей и сил и средств оказания помощи. Для этого первостепенную роль играет получение информации о людях, оказавшихся в опасности, о состоянии окружающей их среды, а также доведение до них информации о тех действиях, которые могут привести к их спасению.

В случае их наличия и работоспособности, сети WLAN могут являться средством, которое потенциально позволяет получать информацию о людях (определение координат, диалог), состоянии среды, передачу информации для координации действий в зоне ЧС.

Однако это не всегда может оказаться возможным, потому необходимо рассмотреть альтернативный сценарий взаимодействия ИУСА с пользователем в случае ЧС. Технологией, которая в таком случае может решить проблему, является гибридная сеть доступа, использующая спутниковый компонент [5]. Спутниковый компонент кардинально повышает доступность и надежность услуги, благодаря меньшей подверженности деструктивным факторам, приводящим к отказам наземной сети.

Гибридная система спутникового доступа

Исторически можно выделить системы фиксированной и мобильной спутниковой связи. Первые применяются, прежде всего, для предоставления транспортных каналов фиксированным абонентам, тогда как вторые – используются в первую очередь для обслуживания мобильных объектов (физических лиц или организаций, транспорта, авиации и судоходства). Мобильные спутниковые службы сосредоточены прежде всего для предоставления услуг мобильной связи конечным пользователям, то есть организуют сеть спутникового радиодоступа. Кроме того, отметим такой режим работы систем спутниковой связи как спутниковый бэкхол (satellite backhaul). До настоящего времени он является основным режимом работы систем спутниковой связи для мобильных операторов.

Долгое время до появления сетей связи третьего (3G) поколения системы спутниковой связи пытались на равных конкурировать с наземными сетями радиодоступа, однако с повсеместным внедрением систем 3G/4G эти решения стали во многом нишевыми. Таким образом сейчас есть класс задач, где спутниковая связь является одной из наиболее надежных и эффективных с точки зрения стоимости решения задачи. Безусловно одной из главных таких задач является связь с удаленными от региональных центров пользователями, находящихся в таких географических условиях, что никакая другая технология не применима. Для условий географии РФ такая задача является типовой для многих возможных сценариев эксплуатации, включая добычу полезных ископаемых, связь в условиях Крайнего севера и многие другие.

Однако в условиях ЧС, возможно прерывание надежной централизованной работы систем стационарной связи, включающих в себя 3G/4G компонент, а потому спутниковый доступ в данном случае может быть рассмотрен как возможное решение для обеспечения задач экстренной связи в интересах ИУСА. При этом для работы ИУСА необходимо обеспечить гибридный доступ к сети, с использованием двух технологий передачи данных.

Под гибридным доступом понимается скоординированное и одновременное использование двух разнородных путей доступа. Так, например, гибридная сеть 4G/5G с использованием спутникового компонента – это такая сеть связи 4G/5G, в инфраструктуре которой используется хотя бы один компонент спутниковой связи, разделенный на космический и земной сегменты. При этом спутниковый сегмент содержит космические аппараты, имеющие на своем борту полезную нагрузку, предназначенную для работы в гибридной сети 5G-6G.

Гибридная спутниковая/наземная система (сеть) [5, 6, 7] – это система, использующая спутниковый и наземный компоненты, в которой спутниковый и наземный компоненты взаимосвязаны, но работают независимо друг от друга. В таких системах спутниковый и наземный компоненты имеют отдельные системы управления сетью и не обязательно работают в одной и той же полосе частот. При этом спутниковый компонент гибридной сети представляет собой комплекс оборудования, позволяющий предоставлять доступ к сетям 4G-6G через космические аппараты.

Системы передачи данных спутникового сегмента могут быть созданы с использованием:

– спутников на низкой околоземной орбите;
– спутников со средней околоземной орбитой;
– спутников с геостационарной околоземной орбитой;
– спутников на высоких эллиптических орбитах.

Работа пользователя в гибридной сети доступа

Практическая реализация прямого взаимодействия пользовательского устройства со спутниковой компонентой возможно только при использовании низкоорбитальных платформ. Такое взаимодействие характеризуется относительно низкой скоростью передачи данных, тем не менее в рамках решаемой задачи (обеспечения связи экстренных служб и ИУСА) характеристики являются приемлемыми.

Спутниковая платформа может быть использована в нескольких возможных ролях:
– ретранслятор,
– базовая станция gNB,
– распределенная базовая станция gNB,
– компонент гибридной сети.

Ниже, на рисунках приведены схематичные иллюстрации различных вариантов использования спутниковой платформы. На рисунке 1 показан сценарий использования спутниковой платформы в типовой роли ретранслятора, тогда как на рисунке 2 приведен один из возможных вариантов использования гибридной схемы.

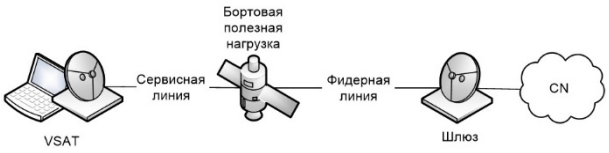

Рис. 1. Сценарий с использованием спутниковой платформы как ретранслятора

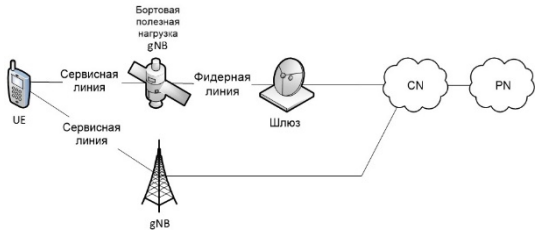

Рис. 2. Сценарий с использованием спутниковой платформы как gNB в гибридной сети

Различные варианты реализации спутниковой компоненты позволяют получить различные показатели использования ресурсов и иные характеристики.

В общем случае, применение гибридной сети доступа влияет на улучшение таких характеристик как:
– обеспечения глобального покрытия,
– пропускной способности,
– надежности,
– уменьшения времени доставки данных,
– повышения доступности услуг.

Показатели качества обслуживания подавляющего большинства современных и перспективных услуг, оказываемых сетями передачи данных под управлением IP протоколов, определены в рекомендациях [8, 9]. В качестве показателя качества предоставления услуги определены вероятностные и временные параметры, отражающие своевременность доставки данных и их достоверность. Наряду с приведенными показателями следует отметить такой показатель как скорость передачи данных [10, 11] между отправителем и получателем данных. Эти показатели должны отражать реальные численные значения оцениваемых параметров в условиях функционирования сети связи, т.е. с учетом обслуживаемого сетью трафика и иных факторов, влияющих на их значения [12].

Доступность услуги

Доступность услуги будем рассматривать как вероятность того, что пользователь, находящийся в произвольной географической точке, может получить услугу ИУСА.

В таблице 1 приведен такой показатель как проникновение – количество пользователей на 100 жителей, а также показатель доступности, вычисленный с использованием метода парных сравнений (экспертных оценок). Статистические данные получены из источников [13-15] и [16].

Проникновение услуг позволяет оценить вероятность того, что у человека, оказавшегося в зоне ЧС, имеется потенциальная возможность использовать ту или иную сеть связи. Показатель доступности позволяет оценить степень доступности связи в любой географической точке.

На рисунке 3 приведена карта с выделением зон доступности сетей операторов сетей подвижной связи [17] (без использования спутникового компонента на уровне доступа).

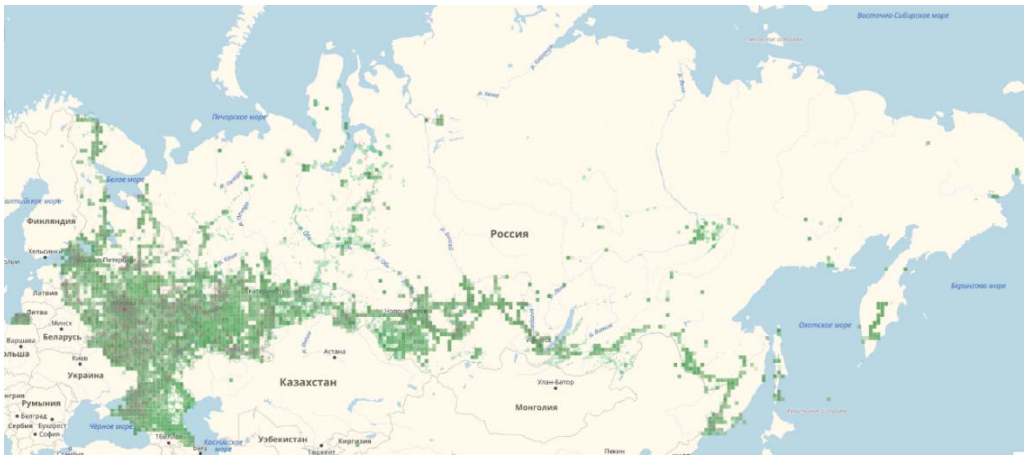

Рис. 3. Доступность ССПС

Таблица 1

Доступность сетей связи

N	Сеть	Проникновение (на 100 жителей)	Доступность
1	ТфОП	19,00	0,000
2	СПС (4/5G)	164,00	0,037
3	БЛВС	*2,50	0,001
4	СПСГ	12,36	0,963

*Значение получено на основе данных о количестве публичных точек доступа из расчета 20 пользователей на одну точку доступа (среднее количество, принимаемое при проектировании подобных сетей).

На рисунке 4 приведены значения данного показателя для различного набора сетей связи. Как видно из гистограммы использование сетей подвижной связи (СПС) и СПСГ (с использованием гибридной сети доступа) позволяет повысить данный коэффициент до величины более 0,999. Включение в комплекс ТфОП и БЛВС увеличивает это значение уже незначительно.

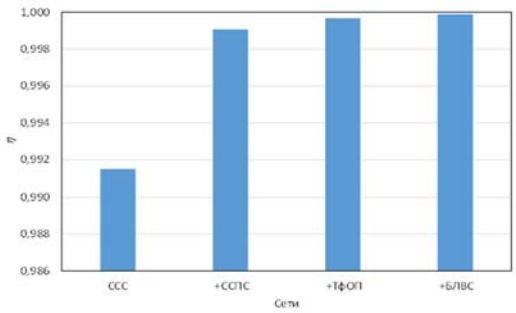

Рис. 4. Зависимость комплексной обобщенной оценки потенциальных возможностей системы связи от используемых сетей

Следует отметить, что исключение гибридной сети доступа из группы сетей приводит к снижению показателя до 0,9882.

Таким образом, можно сделать вывод, что применение гибридных сетей доступа в системе ИУСА обеспечивает наибольший вклад в обеспечение устойчивости и доступности системы в целом.

Заключение

В результате можно отметить, что:

1. Как показывают события, связанные с реагированием в условиях ЧС, наряду с другими возникающими в таких случаях трудностями, задача обеспечения связи как с целью информирования пользователей, так и сотрудников специальных служб должна рассматриваться как приоритетная.
2. Обеспечение связи для задач ИУСА это комплексная задача, решение которой должно быть обеспечено в том числе и в условиях ЧС.
3. Гибридная сеть спутникового доступа может быть рассмотрена как один из перспективных вариантов построения системы передачи данных для нужд ИУСА.

Литература

1. *Sarian Viliam, Nazarenko Anatoly*. Emergency and disaster rescue (EDR). Technical Report: "Network 2030- Additional representative use cases and key network requirements for Network 2030" (June 2020)., Part I.3, pp.16-19.

2. *Сарьян В.К., Парамонов А.И., Викулов А.С., Якубовский Р.М.* Беспроводные локальные вычислительные сети в системе индивидуализированного управления спасениям людей при ЧС // Электросвязь. 2021. № 1. С. 51-59.

3. IEEE Std 802.11-2020. IEEE Standard for Information technology – Telecommunications and information exchange between systems. Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Взамен IEEE Std. 802.11-2016. Введ. 2020. Нью Йорк: Институт IEEE. doi: 10.1109/IEEESTD.2021.9363693. 4379 с.

4. *Парамонов А.И., Сарьян В.К., Горовая Н.В., Лутохин А.С., Саломатина Е.В.* Трафик в системе индивидуализированного управления спасением людей при возникновении ЧС // Электросвязь. 2016. № 5. С. 21-26.

5. TR-348 Hybrid Access Broadband Network Architecture. Issue: 1. Issue Date: July 2016, Broadband Forum, Technical Report.

6. ETSI TR 103 124 Satellite Earth Stations and Systems (SES); Combined Satellite and Terrestrial Networks scenarios V1.1.1, Technical Report, 2013-07.

7. ETSI TR 103 272 Satellite Earth Stations and Systems (SES); Hybrid FSS satellite/terrestrial network architecture for high speed broadband access V1.1.1, Technical Report, 2015-03.

8. ITU-T Y.1540 IP Packet Transfer and Availability Performance Parameters: ITU-T SG12. Series Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities. ITU, 2016.

9. ITU-T Y.1541 Network performance objectives for IP-based services: ITU-T SG12. Series Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities. ITU, 2011.

10. RFC6349 Testing with TrueSpeed from VIAVI Solutions, Application Note.

11. RFC2544 Benchmarking Methodology for Network Interconnect Devices.

12. ФГУП НИИР. Исследования по возможности создания системы персональной спутниковой связи со сплошным покрытием территории России и Арктического региона в полосах частот подвижной службы.

13. Статистика ITU-T. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ITU_regional_global_Key_ICT_ indicator_aggregates_Nov_2020.xlsx (дата обращения 09.09.2021).

14. Статистика ITU-T. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2020/ MobileBroadbandSubscriptions_2007-2019.xlsx (дата обращения 09.09.2021).

15. Статистика ITU-T. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2020/ MobileCellularSubscriptions_2000-2019.xlsx (дата обращения 09.09.2021).

16. *Ямалов И. У*. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций. 4-е изд., электрон. М.: Лаборатория знаний, 2020. 291 с.

17. Роскомнадзор. Карты покрытия территории Российской Федерации услугами подвижной радиотелефонной связи в стандарте GSM 900-1800. URL: https://rkn.gov.ru/communication/p632/ (дата обращения 25.09.2021).

СЕТЬ IOTA КАК СПОСОБ РЕАЛИЗАЦИИ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА В УМНЫХ ГОРОДАХ

Гузаеров Вадим Владиславович,
Московский Технический Университет Связи и Информатики, Москва, Россия

Панков Константин Николаевич,
Московский Технический Университет Связи и Информатики, доцент кафедры «Информационная безопасность», к.ф.-м.н., Москва, Россия
pankov_kn@mtuci.ru

Власов Андрей Викторович,
Московский Технический Университет Связи и Информатики, доцент кафедры «Теория вероятностей и прикладная математика», к.ф.-м.н., доцент, Москва, Россия
pankov_kn@mtuci.ru

Аннотация
В данной статье представлен обзор свойств, которыми должны обладать системы распределённого реестра для их успешного применения в умных городах. Рассказывается о конкретной реализации системы распределённого реестра (сети IOTA), основанной на направленном ациклическом графе, и приводится описание её работы. Делается вывод об оптимальности использования именно сети IOTA при построении умного города по сравнению с традиционным блокчейном.

Ключевые слова: *блокчейн, системы распределенного реестра, интернет вещей, умный город, сеть IOTA, направленный ациклический граф, DAG, информационная безопасность*

Введение

Криптовалюта биткоин и лежащая в ее основе технология блокчейн, получившая в нашей стране названия технологии цепной записи данных [1] или сквозной цифровой технологии системы распределенных реестров [2], последние годы является источником обсуждений и споров как в деловых, так и в научных кругах. По мнению ее сторонников, технология распределенных реестров (Distributed Ledger Technology, или DLT) является ключевой технологией 21 века, которая по-новому раскроет такие понятия, как торговля, защита персональных данных, демократизация общества и устранит необходимость в центральных регуляторах во многих других областях [3]. Противники же считают, что огромный ажиотаж вокруг технологии не обоснован, а сама технология не более чем средство для спекуляции и других форм незаконной деятельности, основанных на анонимности [4].

Хотя раскол в представлениях о технологиях распределенных реестров является значительным, большинство современных исследователей согласны с одним основным фактом - технология распределенных реестров потенциально является очень наукоёмкой технологией. Грубо говоря, как следует из названия, технология распределенных реестров – это технология хранения и обработки информации, ключевыми особенностями которой является совместное использование и синхронизация цифровых данных. Несколько распределенных владельцев этого реестра достигают консенсуса, чтобы согласовать содержание реестра и управлять им таким образом, чтобы он не мог быть изменен. Такой реестр может использоваться не только для отслеживания финансовых операций, но и для записи того "кто, что и когда сделал" в целом ряде нефинансовых приложений. Опираясь на большой класс таких систем, в которых люди и машины (вычислительные устройства), или машины и другие машины, должны согласовывать свое поведение для достижения общей цели, в современном научном сообществе есть заинтересованность в использовании технологий распределенных реестров в качестве инструмента синхронизации. Поэтому объектом исследования данной работы является изучение конкретной реализации технологии распределённого реестра (сети IOTA) [5] для решения проблем, возникающих в контексте умных городов.

Сеть IOTA – это открытая масштабируемая система распределённого реестра, которая использует технологию DAG (направленный ациклический граф) [6]. Она помимо криптовалютного сектора также применяется в статистике, машинном обучении и разработках, связанных с искусственным

интеллектом [7]. В сети IOTA нет комиссий – отправка монеты абсолютно бесплатна, что делает технологию привлекательной для использования в сфере интернета вещей, где множество устройств должны будут одновременно отправлять тысячи микротранзакций различной природы.

Под умным городом в настоящее время принято понимать концепцию интеграции нескольких информационных и коммуникационных технологий и решений Интернета вещей для управления городским имуществом, которые используются для повышения качества, производительности и интерактивности городских служб, снижения расходов и потребления ресурсов, улучшения связи между жителями города и муниципалитетом. В период до 2024 года в Российской Федерации действует проект «Умный город», реализуемый в рамках национального проекта «Жилье и городская среда» и национальной программы «Цифровая экономика» [8].

Системы распределенных реестров и концепция умного города

Заметим, что применению систем распределенного реестра в системах интернета вещей, тесно связанных с умным городом, в последние годы посвящен целый ряд работ, к примеру [9].

В настоящее время существует также достаточно большое количество работ, посвященных использованию технологии блокчейна непосредственно в концепции умного города, к примеру [10], [11], [12]. В этих работах рассматриваются как концептуальные основы внедрения технологии, так и существующие примеры успешного внедрения.

Системы распределенного реестра, несмотря на концептуальную простоту, должны обладать определенными свойствами, чтобы быть полезными при решении крупномасштабных задач в контексте умных городов.

– Архитектура системы распределенного реестра должна быть масштабируемой. То есть, для приложений интернета вещей количество транзакций в секунду между устройствами может исчисляться тысячами. Поэтому система должна быть способна управлять таким количеством операций.

– Двойное расходование. Инфраструктура системы распределенного реестра должна быть устойчива к атакам со стороны злоумышленников (например, структура должна быть защищена от атак на двойное расходование). Здесь под двойным расходованием мы подразумеваем способность агента потратить один и тот же токен более одного раза.

– Энергетические затраты. Поскольку стоимость энергии, которая тратится для майнинга 1 блока в блокчейне биткоина, уже приближается согласно оценкам многих специалистов к абсурдному уровню, затраты на энергию для поддержания сетевой инфраструктуры в стабильном состоянии и защиты от атак должны поддерживаться на разумном уровне.

– Комиссии. Транзакции должны быть свободны от транзакционных издержек. Это чрезвычайно важная характеристика для сетей с большим количеством устройств транзакций.

Отметим, что применение систем распределенного реестра при построении системы умного города является одним из способов обеспечения его информационной безопасности. Однако, в связи с наличием криптографических механизмов, которые используются при построении блокчейн систем, при выполнении требований законодательства Российской Федерации возникает задача сертификации подобных комплексов умных городов [13], что усложняет их внедрение на практике. Также остается открытой задача тестирования верификации и валидации подобных систем [14] как отдельного инструмента обеспечения информационной безопасности.

Архитектуры систем распределенных реестров

В этом разделе приведем описания двух широко используемых архитектур систем распределённого реестра - традиционного блокчейна и систем, использующих направленный ациклический граф.

А. Традиционный блокчейн

Блокчейн был впервые представлен Сатоши Накамото в его фундаментальной работе [15] как технология, на основе которой был разработан Биткойн. С момента появления этого первого документа и после успеха Биткойна было разработано большое количество других валют, пытающихся имитировать или улучшить первоначальный дизайн. Почти все эти валюты в своей основе имеют одну и ту же архитектуру.

Блокчейн – это одноранговая распределенный реестр транзакций, что означает, что реестр не хранится на центральном сервере, а его копии распределены по сети частных компьютеров (узлов). Для обмена валютой (или информацией) узлы осуществляют транзакции между собой, используя криптографию с открытым/закрытым ключом. Каждый владелец счета имеет открытый ключ и секретный ключ. Последний используется для подписания/аутентификации транзакций, в то время как открытый

ключ обеспечивает уникальный адрес в системе [16, 21]. Консенсус обеспечивается с помощью технологии доказательства выполнения работы (Proof of Work).

B. Направленные ациклические графы (Directed Acyclic Graph, DAG)

В другом решении для достижения консенсуса используется направленный ациклический граф, который является основой нескольких криптовалют (например, IOTA, Byteball Nano). Другими словами, это граф, состоящий из конечного числа вершин и ребер, причем каждое ребро направлено от одной вершины к другой так, что не существует пути, соединяющего вершину v с самой собой.

Пример направленного ациклического графа изображен на рисунке 1. Обратим внимание, что технически граф, изображенный на рисунке 1, содержит один цикл (то есть вершины 2, 4, 5, 10), но ребра, соединяющие одну вершину с другой, направлены только в одну сторону, поэтому невозможно найти путь от любой вершиной до неё самой.

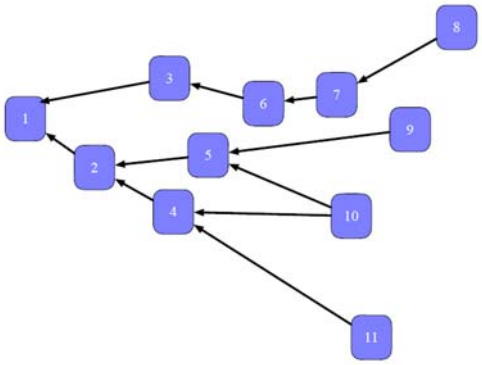

Рис. 1. Пример направленного ациклического графа с 11 вершинами и 10 ребрами.

Частным случаем системы распределенного реестра с направленным ациклическим графом является IOTA Tangle (с англ. – «клубок», «запутывание»). Заметим, чтотangle в IOTA в просторечии часто является синонимом DAG. Целью создания Tangle, согласно оригинальной статье [17], является разработка криптовалюты для индустрии интернета вещей, основными характеристиками которой являются отсутствие комиссий и низкое энергопотребление. По сути, Tangle представляет собой направленный ациклический граф, где каждая вершина представляет собой транзакцию, в то время как граф представляет собой реестр. Всякий раз, когда выпускается новая транзакция, она должна одобрить две предыдущие транзакции. Каждое одобрение представляет собой ребро графа. Еще не одобренные транзакции именуются tip. Направленное ребро между транзакцией i и транзакцией *j* означает, что *i* напрямую одобряет *j*, тогда как если существует путь (но не одно ребро), соединяющий *i* с *j*, мы говорим, что *j* косвенно одобрен *i* (например, см. рис. 2). Первая транзакция в Tangle называется генезис-блоком, и все транзакции косвенно одобряют ее.

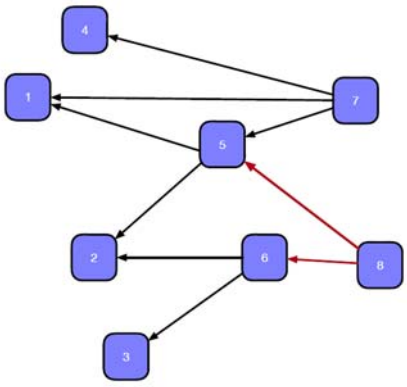

Рис. 2. Транзакция 8 напрямую одобряет 5 и 6, косвенно одобряет 1, 2 и 3 и не одобряет 4 и 7.

Чтобы лучше понять предыдущий процесс, обратимся к рисунку 3: здесь представлен определенный экземпляр Tangle с тремя новыми входящими транзакциями (верхняя панель). Зеленый блок – это

блок генезиса, синие блоки – это транзакции, которые уже были одобрены, красные блоки представляют собой текущие вершины Tangle, а серые блоки – это новые входящие транзакции (tips). Сразу же после выпуска новый транзакции пытается прикрепиться к двум из текущих кончиков сети (средний граф). Если какая-либо из выбранных неподтверждённых транзакцией не согласуется с предыдущими транзакциями или друг с другом, выбор будет отклонен и будут выбраны две другие неподтверждённые транзакции. Обратите внимание, что на данном этапе эти транзакции еще не являются частью Tangle, поскольку они выполняют необходимую работу (Proof of Work). Они остаются неподтвержденными (пунктирные линии), пока этот процесс не закончится. После завершения работы, выбранные входящие транзакции становятся подтвержденными транзакциями, а серые блоки добавляются в набор новых входящих (нижний граф).

В отличие от традиционного блокчейна, в котором все блоки записываются один за другим, в Tangle все транзакции записываются без последовательности – то есть они все могут обрабатываться одновременно, а не последовательно одна за другой. Это позволяет Tangle-сетям проводить транзакции быстрее и эффективнее, чем это делают обычные системы распределенного реестра [18].

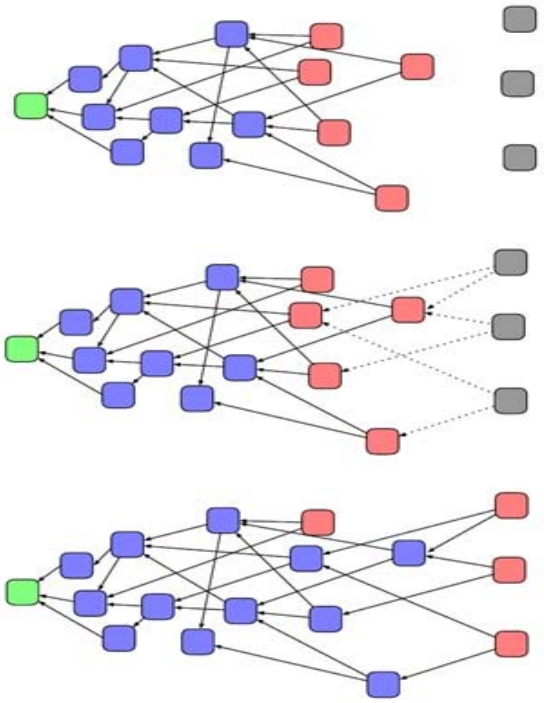

Рис. 3. Последовательность выпуска новой транзакции. Зеленый участок представляет генезис блок, синие участки представляют одобренные транзакции, а красные - новые входящие транзакции. Сплошные линия представляют одобрения в сети, а пунктирные – транзакции, выполняющие работы для одобрения двух новых входящих транзакций

В соответствии с [19] использование именно систем распределенного реестра, использующих направленный ациклический граф, поведение которого описывается с использованием цепей Маркова [20], позволяет добиться выполнения свойств, которые актуальны при решении крупномасштабных задач в контексте умных городов.

Заключение

Таким образом, результатом данной работы можно признать то, что системы распределенного реестра остаются актуальным предметом научных исследований в контексте их применения в различных областях. В рамках данной работы были проанализированы свойства, которыми должны обладать блокчейн системы, чтобы быть полезными при решении крупномасштабных задач в контексте умных городов, в том числе и с точки зрения информационной безопасности. Были рассмотрены основные архитектуры существующих систем распределенного реестра, в частности, была описана архитектура и принцип работы сети IOTA, которая была признана более подходящей для применения в системе умного города по сравнению с традиционным блокчейном.

Литература

1. Методические рекомендации ТК-26 МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров».
2. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // Электрон. дан. Заглавие с экрана. Режим доступа: https://digital.gov.ru/uploaded/files/07102019srr.pdf
3. Walport M.G.C.S.A. Distributed ledger technology: Beyond blockchain. UK Government Office for Science, 1 Victoria Street London SW1H 0ET, No. GS/16/1, 2016 // Электрон. дан. Заглавие с экрана. Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
4. *Gatteschi V., Lamberti F., Demartini C., Pranteda C., Santamaría V*. To Blockchain or Not to Blockchain: That Is the Question // IT Professional, vol. 20, no. 2, 2018, pp. 62-74.
5. *Silvano W.F., Marcelino R.* Iota Tangle: A cryptocurrency to communicate Internet of Things data // Future Generation Computer Systems, 112, 2020, pp. 307-319.
6. *Müller S., Penzkofer A., Polyanskii N., Theis J., Sanders W., Moog H*. Tangle 2.0 Leaderless Nakamoto Consensus on the Heaviest DAG // IEEE Access, vol. 10, 2022, pp. 105807-105842.
7. *Lee J., Kim W.* DAG-Based Blockchain Sharding for Secure Federated Learning with Non-IID Data // Sensors 2022, 22, pp. 8263.
8. Проект Цифровизации городского хозяйства «Умный город». МинСтрой Росии. Электрон. дан. Заглавие с экрана. Режим доступа: https://www.minstroyrf.gov.ru/trades/gorodskaya-sreda/proekt-tsifrovizatsii-gorodskogo-khozyaystva-umnyy-gorod/
9. *Панков К.Н., Эйнман А.Д.* Исследование технологии системы распределенного реестра в системе промышленного Интернета вещей с точки зрения информационной безопасности // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13. № 2. С. 33-40.
10. *Парменова Н.* Госуслуги на блокчейне. Как будут жить города будущего. 06.02.2018. Электрон. дан. Заглавие с экрана. Lee, J.; Kim, W. DAG-Based Blockchain Sharding for Secure Federated Learning with Non-IID Data. Sensors 2022, 22, 8263. https://doi.org/10.3390/s22218263
11. «Умные города» на основе технологии блокчейн. 02.03.2018. Электрон. дан. Заглавие с экрана. Режим доступа: https://cryptocartel.club/ru/blokcheyn/umnye-goroda-na-osnove-tehnologii-blokcheyn
12. *Гриценко В.П., Штомпель Л.А*. От smart city к blockchain city: в поисках образа идеального города // Культурная жизнь Юга России. 2018. № 3(70). С. 12-17.
13. *Панков К.Н., Эйнман А.Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 37-49.
14. *Pankov K.N.* Testing, Verification and Validation of Distributed Ledger Systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19-20 марта 2020 года. P. 9078541.
15. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Электрон. дан. Заглавие с экрана. Режим доступа: https://bitcoin.org/bitcoin.pdf.
16. *Панков К.Н*. Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества : Материалы XII Международной отраслевой научно-технической конференции, Москва, 14-15 марта 2018 года. С. 365-366.
17. *Popov S*. The Tangle-Version 1.4.3. IOTA Whitepaper. Электрон. дан. Заглавие с экрана. Режим доступа: https://www.allcryptowhitepapers.com/iota-whitepaper/
18. Обзор IOTA и MIOTA: сможет ли проект снова выбиться в лидеры рынка? 25.03.2022 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://media.sigen.pro/reviews/10205
19. *Conti M., Kumar G., Nerurkar P., Saha R., Vigneri L.* A survey on security challenges and solutions in the IOTA // Journal of Network and Computer Applications. Vol. 203, 2022, pp. 103383.
20. *Wirth F., Stuedli S., Yu J., Corless M., Shorten R*. Nonhomogeneous Markov Chains, unsynchronised AIMD, and Optimization // Journal of the ACM, Vol. 66, Issue 4, 2019, pp. 1-37.
21. *Панков К.Н.* Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4-18.

ПРИМЕНЕНИЕ МЕТОДА SRMD ДЛЯ РЕСТАВРАЦИИ КОНТЕНТА ДЛЯ СЕРВИСА ПОТОКОВОГО ВЕЩАНИЯ

Киселева Александра Сергеевна,
Московский Технический Университет Связи и Информатики, магистр, Москва, Россия
alexandra.080600@gmail.com

Власюк Игорь Викторович,
Московский Технический Университет Связи и Информатики, к.т.н., доцент каф. ТиЗВ, Москва, Россия,
ru3dlp@yandex.ru

Аннотация
Выбор эффективного метода реставрации качества видео для сервисов Over-The-Top (OTT) является сложной задачей в настоящее время. Становится непросто обеспечить приемлемое качество восприятия (QoE) для пользователей, из-за чего появляется необходимость в подборе наиболее эффективного метода повышения качества предоставляемого контента. В данной статье представлен обзор метода реставрации качества SRMD. В обзоре кратко описаны способ работы сервисов OTT и метода SRMD, а также проведен сравнительный анализ с другими популярными методами повышения качества.

Ключевые слова: *Реставрация качества видео, OTT-сервис, QoE, SRMD, оценка качества видео, потоковое вещание.*

Введение

Использование мультимедийных услуг сильно возросло за последние годы. Это вызвано растущей популярностью и использованием услуг потокового вещания (например, YouTube и Netflix), которые привели к появлению новых возможностей для получения прибыли для интернет-провайдеров (ISP), мобильных операторов и провайдеров Over-The-Top (OTT).

Важной задачей для дальнейшего успеха таких услуг является обеспечение высокого качества видео для конечных пользователей [1]. Достижение хорошего качества обслуживания (QoE) является сложной задачей из-за многих факторов, таких как изменяющееся медиа-содержимое, изменяющиеся условия передачи, а также значительные пространственные и временные изменения в производительности сетей распространения контента (CDN). Наиболее распространенные механизмы, используемые для улучшения QoE конечных пользователей, основаны либо на оптимизации сети, либо на адаптивной передаче видеопотока, управляемой клиентом. Несмотря на это, управление QoE все равно остается сложной задачей [2, 15-19] из-за множества проблем, которые можно разделить на четыре различных аспекта:

1. Изменчивость сетевых ресурсов, нестабильная природа беспроводных каналов и характеристики фиксированных/мобильных сетей в гетерогенной среде. Перегруженные места, такие как поезда, стадионы и торговые центры, требуют постоянной адаптации распределения сетевых ресурсов для клиентов.
2. Появление новых услуг (например, виртуальной/дополненной реальности (VR/AR)), ожидания пользователей в сочетании с оптимизацией операционных затрат мобильных и сервисных провайдеров.
3. Разнообразие сетей (например, фиксированных и мобильных), в которых для управления QoE необходимо использовать различные методы измерения и оценки с учетом ограничений ресурсов.
4. Популярность и быстрый рост мультимедийных услуг в Интернете и разнообразие устройств конечных пользователей с различными возможностями (например, размер экрана, вычислительная мощность/ресурсы и возможности хранения).

Технология OTT

Согласно словарю OTT-терминов от Минкомсвязи России, OTT (от англ. Over the Top) — это метод (формат), с помощью которого информация, набор данных (цифровой контент, файлы), разбивается на IP пакеты и доставляется от одного компьютера к другому по неуправляемой сети Интернет (по сетям

сторонних операторов связи) от источника к получателю. Проще говоря, технология OTT (аббр. от англ. Over the Top) – это метод предоставления видеоуслуг через Интернет.

Благодаря OTT производится доставка видеосигнала от провайдера на устройство пользователя, такие как приставка, компьютер и мобильный телефон, по сетям передачи данных [3]. Использование OTT возможно без прямого контакта с оператором связи в отличие от традиционных услуг IPTV, которые в основном предоставляются только через управляемую самим оператором сеть с гарантированным качеством обслуживания (QoS),

OTT использует IP как сеть передачи данных. Трафик передается через HTTP и TCP на транспортном уровне. Таким образом, OTT представляет собой веб-сервер с файловым хранилищем (аналогично FTP). Для получения файла с сервера клиентское устройство, использует команду GET протокола HTTP. Однако видеопоток не может быть передан в виде одного файла. Чтобы решить эту проблему, ТВ-контент разделен на множество сегментов/блоков, каждый из которых представляет собой аудио – и видеодорожку.

Обычно размещается несколько версий контента с разной степенью сжатия для предоставления услуги независимо от ширины канала и скорости передачи на сервере. Так как качество связи периодически меняется, используется постоянный мониторинг изменения условий передачи или доставка запросов о пропускной способности канала, а плеер управляет буферизацией таким образом, что смена скорости никак не сказывается на непрерывности воспроизведения картинки.

Для каждой видеоуслуги создается манифест-файл с информацией о доступных скоростях передачи. До того, как запросить видео, клиент получает манифест-файл, выбирает подходящую скорость передачи и затем запрашивает загрузку сегментов, содержащих видео, кодированное с выбранной скоростью.

Метод измерения QoE

В прошлом для определения уровня удовлетворенности услугой пользователем использовались измерения на основе качества обслуживания (QoS), учитывающие параметры сети, таких как потеря пакетов, задержка и пропускная способность. В этом случае впечатления абонента формирует производительность и стабильность сети, наличие/отсутствие артефактов при просмотре видео, а также посторонних шумов в разговорах по VoIP. Поскольку метрики QoS не имеют явной и прямой связи с удовлетворенностью клиента услугой, в последние годы для оценки качества мультимедийных услуг в дополнение к метрикам QoS стала использоваться ориентированная на пользователя оценка Quality of Experience (QoE) (например, Mean Opinion Scores (MOS)).

QoE – дословно «качество восприятия» или степень удовлетворенности пользователя. QoE учитывает субъективное отношение пользователя к конкретной услуге, которое можно определить как степень удовлетворенности от приложения или услуги [4]. С недавних пор используется в телекоммуникационной терминологии и, учитывая субъективное отношение пользователя к конкретной услуге, определяет степень удовлетворенности конечного пользователя услугами, предоставляемыми провайдером связи. Факторы, которые влияют на QoE, представлены на рисунке 1.

Часть факторов, влияющих на QoE, субъективны, но, несмотря на это, качество восприятия пользователей можно измерить. В этой области идет большое количество исследований. Метод определения зависит от сервиса или услуги (аудио, видео, стриминг и др.). На субъективную оценку пользователя влияет его опыт работы с другими операторами. Он сравнивает цены, отношение технической поддержки и так далее.

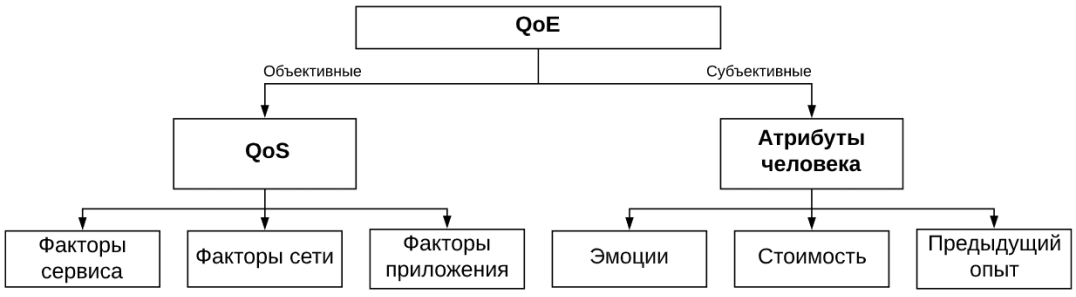

Рис. 1. Факторы, влияющие на QoE

Характер искажений определяется ошибками преобразования и доставки контента, которые могут возникать на любом участке процесса OTT. Такие ошибки приводят к нарушению целостности изображения, как во времени, так и в пространстве.

Основные проявления временных искажений:

- мерцание яркости или цвета (особенно заметны мелкозернистое и крупнозернистое мерцание);
- затуманивание и/или мерцание на резких границах переднего и заднего планов;
- кажущееся движение переднего плана относительно заднего;
- дрожание изображения, обусловленное дискретизацией кадров.

Основные проявления пространственных искажений:

- «размытие» деталей, обычно на резких краях изображений;
- ореол или шлейф на резких границах изображений;
- «просачивание» и наложение цветов на краях объектов изображения;
- шум в виде ступенек на диагональных и искривленных краях объектов изображения.

Процесс управления и оптимизации QoE конечных пользователей требует знаний о первопричине ухудшения QoE или неудовлетворительного уровня QoE. В этом отношении необходимо отслеживать, собирать и измерять соответствующую информацию и данные, относящиеся к возможностям оборудования (например, размер экрана, производительность дисплея), информацию о конкретном приложении или услуге и ее количественную оценку, информацию о QoE внутри сети. Параметры сети, а также информация о битовом потоке могут быть собраны с клиентских устройств или элементов сети. Собранные ключевые показатели производительности (KPIs) на уровне сети, например, пропускная способность, потеря пакетов, задержка или ключевые показатели качества (KQIs) на уровне услуг, например, частота кадров, разрешение видео, удобство использования услуг и надежность, являются исходными данными для моделей оценки QoE [5].

Стандарты для адаптивных потоковых решений.

Большая часть видеотрафика Интернета сегодня передается через HTTP Adaptive Streaming (HAS) [6]. К преимуществам HAS [7] относятся:

- обеспечение надежной передачи,
- возможность повторного использования инфраструктуры кэша,
- возможность обхода брандмауэра.

Основываясь на этих преимуществах, HAS был принят на коммерческой основе Microsoft Smooth Streaming, Adobe Dynamic Streaming, Netflix и Apple HTTP Live Streaming для услуг потоковой передачи мультимедиа. HAS широко используется в OTT сервисах, таких как Netflix и YouTube, как стандарт для адаптивных потоковых решений. Решения HAS [6] используют надежные механизмы доставки, такие как TCP и Quick UDP Internet Connections (QUIC). Однако из-за несоответствия этих собственных решений HAS и форматов 3GPP появился стандарт динамической адаптивной потоковой передачи данных по HTTP (DASH). Рисунок 2 иллюстрирует концепцию DASH, предполагающую метод адаптации скорости видео (например, на основе пропускной способности, на основе буфера или гибридный) для потокового видео.

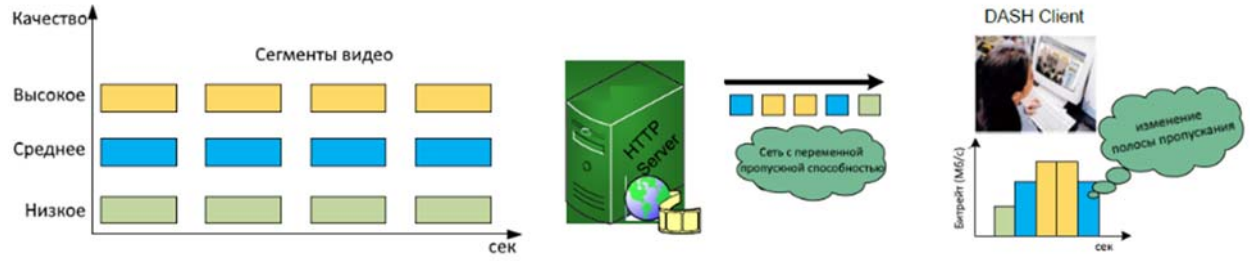

Рис. 2. Динамическая адаптация в зависимости от условий сети.

Видео кодируется на различных уровнях представления (пространственном/временном/качественном), затем делится на фрагменты с одинаковой продолжительностью, которые хранятся на сервере. Когда пользователь делает первый запрос на видеофайл, сервер отправляет соответствующий файл манифеста, который состоит из подробной информации о видеофайле, такой как продолжительность, размер сегмента, уровни представления или тип кодека [7].

Затем происходит измерение текущей полосы пропускания и состояния буфера, после запрашивается следующая часть сегмента видео с соответствующим битрейтом. Таким образом, количество и продолжительность задержек может быть уменьшена, а доступная полоса пропускания будет использоваться наилучшим образом. DASH обеспечивает доставку медиапотоков как в режиме реального времени, так и по запросу через HTTP.

Несмотря на децентрализованный характер принципа HAS, все еще существуют некоторые недостатки, связанные с нестабильностью видео из-за переключения битрейта и недостаточным использованием сетевых ресурсов [8]. Эти проблемы остаются серьезной проблемой для поставщиков видеоконтента и сетевых операторов. Для решения этих проблем существует стандарт MPEG-SAND, в котором используются централизованные узлы в сети для улучшения доставки контента DASH [9].

DASH с использованием сервера и сети (SAND) является расширением стандарта MPEG-DASH, который был доработан для улучшения доставки контента DASH. Спецификация SAND вводит сообщения между клиентом DASH и сетевыми элементами или между различными сетевыми элементами. Сообщения SAND улучшают сеанс потоковой передачи, предоставляя информацию о рабочих характеристиках сетей, серверов, прокси-серверов, кэша, CDN в реальном времени, а также о производительности клиента DASH.

Метод реставрации качества Super resolution network for Multiple Degradations (SRMD)

С развитием технологий и повышением производительности аппаратуры в последние годы высокую скорость и эффективность получила архитектура сверточных нейронных сетей (CNN). Для решения задач компьютерного зрения в 2018г. был разработан метод Single-image super-resolution (SISR), который восстанавливает изображение с высоким разрешением (HR) из изображения с низким разрешением (LR) на основе CNN,

Существующий метод SISR предполагает, что изображение с низким разрешением подвергается бикубическому понижению дискретизации из изображения с высоким разрешением. В ситуации, когда истинное ухудшение качества изображения не следует этому предположению, отмечается снижение производительности даже на современном аппаратном обеспечении (с поддержкой CUDA и DLSS). Кроме того, методу не хватает масштабируемости при обработке множественных участков пониженного качества в кадре.

Алгоритм SRMD (Super resolution network for Multiple Degradations) [10] является вариантом SISR, обеспечивающим восстановление изображения с низким разрешением (LR) в высокое (HR) в множественных областях понижения качества.

В качестве входных данных SRMD принимает изображение LR и карты деградации. Каскад сверточных слоев 3×3 применяется для выполнения нелинейного отображения. Каждый уровень состоит из трех типов операций, включая свертку (Conv), ReLU и пакетную нормализацию (BN). Наконец, за слоем субпиксельной свертки, следует последний сверточный слой для преобразования нескольких частичных изображений HR.

Описание набора исходных данных

В качестве исходного материала для повышения качества было взято видео MeridianConversation_VMAF-ViterbiQualityBasedAdaptor_Trace_0.mp4 (рис. 3) из базы LIVE_NFLX_Plus [11], [12] со следующими параметрами:

- Разрешение: 1920x1080@30,
- Битрейт: 6343 кб/с.,
- Кодек: h264,
- Длительность: 00:00:27,
- Количество кадров: 808.

Рис. 3. Иллюстрация используемой видеопоследовательности «Meridian Conversation».

Реставрация качества видео

Для выполнения данной работы использовался алгоритм SRMD, с помощью которого произведена реставрация качества видео, а также методы бикубической интерполяции и RealSR были выбраны для сравнения. Кадры, по которым можно визуально оценить изменение качества видео после обработки, представлены на рисунке 4.

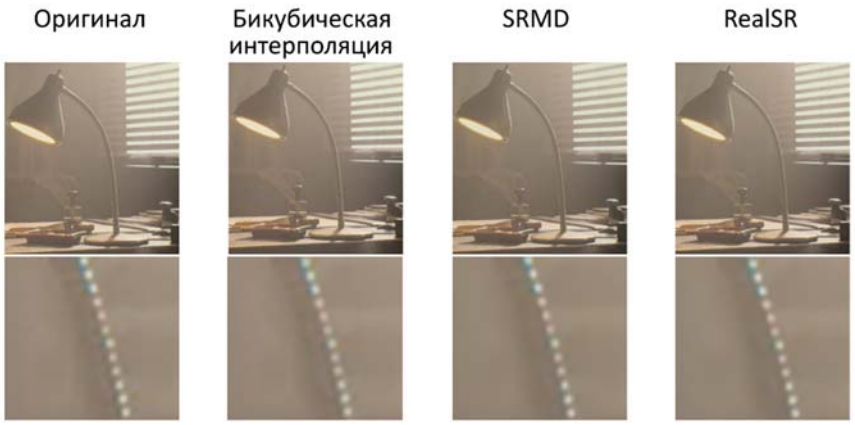

Рис. 4. Фрагменты кадра.

Длительность обработки видео методом бикубической интерполяции составила 1448 с, методом SRMD – 5355 с и методом RealSR – 3785 с.

Субъективная оценка качества

Анализ качества видео производился безреференсной метрикой NIQE. Безреференсная метрика позволяет оценить качество видео без какой-либо информации об эталонном видео с помощью алгоритма, в котором единственной входной информацией является искаженное видео, качество которого оценивается.

Рассмотренная метрика осуществляют покадровую оценку качества видео, соответственно не имеет временной модели. Для учета временных характеристик зрительной системы человека [13] предлагается осуществить свертку значений метрик с временной импульсной характеристикой зрения по формуле (1).

$$M_p(n) = \sum_{n_c}^{N-1} M(n - n_c) \times V(n_c) \quad (1)$$

M - значение метрики;

$V(n_c)$ - импульсная характеристика зрительной системы человека;

N - число отсчетов $V(n_c)$;

n - текущий кадр.

Временную импульсную характеристику зрения (рис. 5) для вычисления найдем путем дискретизации характеристики [14] с периодом, равным частоте кадров тестовой видеопоследовательности. Временная фильтрация отсчетов метрики, а не исходной видеопоследовательности является корректной при условии, что значение метрики линейно зависит от субъективного качества видеопоследовательности или, если указанное условие не выполняется в случае, когда изменение оценок в пределах окна фильтрации достаточно мало. Мы считаем, что в нашем случае, по крайней мере, одно из указанных выше условий выполняется.

В результате фильтрации значений метрик получен график зависимости их значений от времени (номера кадра). На рисунке 6 показаны значения метрики оценки качества видео до и после реставрационной обработки видео.

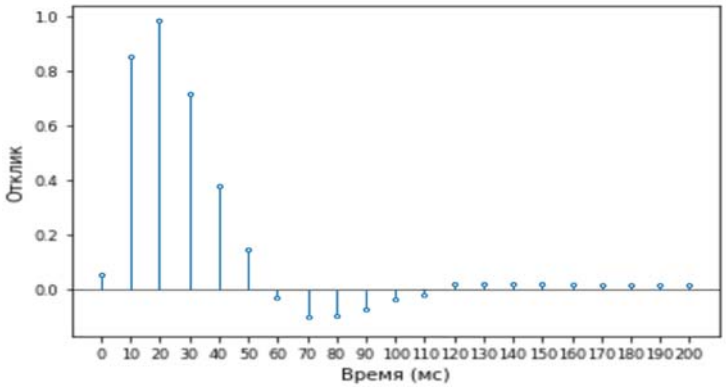

Рис. 5. Временная импульсная характеристика зрения.

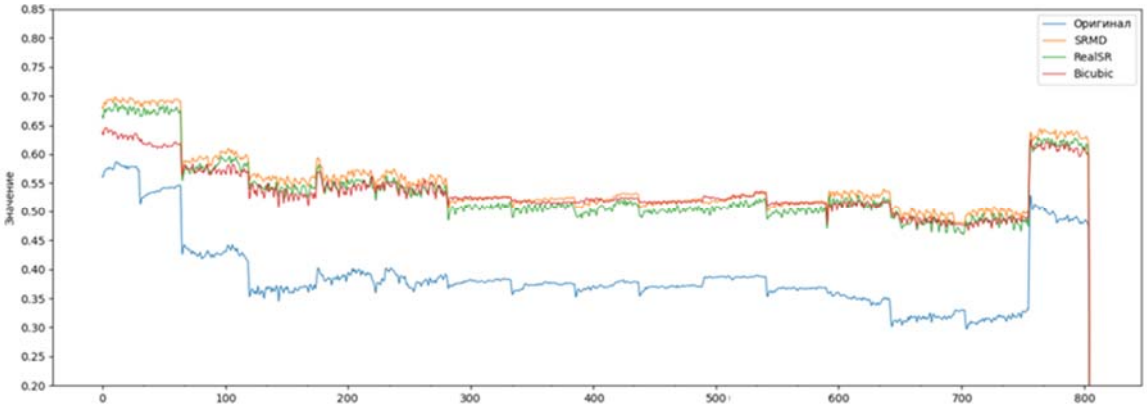

Рис. 6. График оценки качества видео метрикой NIQE

В дальнейшем, при реализации метода, предполагается, что предварительная оценка качества видео будет формировать сигнал управления для включения процедуры реставрационной обработки, таким образом, процедуре восстановления будут подвергаться только временные фрагменты, качество которых соответствует значениям метрики ниже пороговых.

Заключение

В данной работе был рассмотрен такой метод реставрации качества видеопоследовательности в сервисах OTT, как SRMD. Был произведен сравнительный анализ с методами бикубической интерполяции и RealSR с помощью безреференсной метрики оценки качества видеопоследовательности NIQE.

Результаты показали, что SRMD является эффективным методом повышения качества и масштабирования видеокадров. В частности, в сравнение с методами бикубической интерполяции и RealSR метод SRMD показал наилучший результат. Субъективную оценку качества видеопоследовательности дает метрика NIQE: в среднем качество видеопоследовательности было повышено на 15%. Визуальная оценка качества видео последовательности показала, что SRMD может не только удалять неудовлетворительные артефакты, но и создавать острые края, также SRMD может восстанавливать четкое изображение с лучшей интенсивностью. Однако отрицательной стороной является относительно низкая

производительность метода: 1 кадр в секунду без использования специализированного видеоускорителя. Длительность обработки видеопоследовательности методом SRMD составляется 5355 с, что превышается длительность работы метода бикубической интерполяции на 270%, а метода RealSR – на 41%.

Литература

1. Rivera D., Kushik N., Fuenzalida C., Cavalli A., Yevtushenko N. QoE Evaluation based on QoS and QoBiz Parameters applied to an OTT service // IEEE International Conference on Web Services, (New York, NY, USA), pp. 57-64, 2015.
2. Barakovi´c S., Skorin-Kapov L. Survey and Challenges of QoE Management Issues in Wireless Networks // Journal of Computer Networks and Communications, vol. 2013, pp. 1-28, Dec 2013.
3. *Топильский С.А., Власюк И.В*. OTT телевидение как развитие интернет вещания // Телекоммуникации и информационные технологии. 2015. Т. 2, № 1. С. 59-61. EDN WHMCAV
4. "ITU-T Rec. P.10/G.100: Vocabulary for performance and quality of service. Amendment 5: New definitions for inclusion in Recommendation ITU-T P.10/G.100," July 2016.
5. *Robitza W., Ahmad A., Kara P.A., Atzori L., Martini M.G., Raake A., Sun L*. Challenges of future multimedia QoE monitoring for internet service providers // Multimedia Tools and Applications, pp. 1-24, June 2017.
6. *Barman N., Martini M.G.* QoE Modeling for HTTP Adaptive Video Streaming-A Survey and Open Challenges // IEEE Access, vol. 7, pp. 30831-30859, March 2019.
7. *Seufert M., Egger S., Slanina M., Zinner T., Hoßfeld T., Tran Gia P.* A Survey on Quality of Experience of HTTP Adaptive Streaming // IEEE Communications Surveys & Tutorials, vol. 17, pp. 469–492, First quarter 2015.
8. *Rodríguez D.Z., Wang Z., Rosa R.L., Bressan G.* The impact of video-quality-level switching on user quality of experience in dynamic adaptive streaming over HTTP // EURASIP Journal on Wireless Communications and Networking, vol. 2014, no. 1, 2014.
9. *Cofano G., Cicco L.D., Zinner T., Nguyen-Ngoc A., Tran-Gia P., Mascolo S.* Design and Experimental Evaluation of Networkassisted Strategies for HTTP Adaptive Streaming // ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 35, pp. 1-24, Nov 2017.
10. *Zhang Kai, Zuo Wangmeng, Zhang Lei.* Learning a Single Convolutional Super-Resolution Network for Multiple Degradations. Proceedings / CVPR, IEEE Computer Society Conference on Computer Vision and Pattern Recognition. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2018.
11. *Bampis C G., Li Z., Katsavounidis I., Huang T., Ekanadham C., Bovik A.C*. Towards Perceptually Optimized End-to-end Adaptive Video Streaming, submitted to IEEE Transactions on Image Processing: a Publication of the IEEE Signal Processing Society, 2018, pp. 2-5.
12. *Mozhaeva A., Potashnikov A., Vlasuyk I., Streeter L*. Constant Subjective Quality Database: The Research and Device of Generating Video Sequences of Constant Quality // 2021 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2021, pp. 1-5, doi: 10.1109/EMCTECH53459.2021.9618977.
13. *Mozhaeva A.I., Vlasuyk I.V., Potashnikov A.M., Cree M.J., Streeter L*. The Method and Devices for Research the Parameters of the Human Visual System to Video Quality Assessment // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, 2021, pp. 50.
14. *Tong J., Ramamurthy M., Patel S.S., Vu-Yu L.P., Bedell H.E*. The temporal impulse response function during smooth pursuit. Vision Res. 2009 Nov;49(23):2835-42. doi: 10.1016/j.visres.2009.08.019. Epub 2009 Aug 23. PMID: 19706304; PMCID: PMC2783465.
15. *Vyatkin M., Potashnikov A., Selivanov V., Vlasuyk I., Nezhivleva K., Mozhaeva A.* Method of preventing leakage of personal data through eyetracking modules of user devices // T-Comm: Телекоммуникации и транспорт, 2022. Т. 16. № 7. С. 44-51.
16. *Mozhaeva A., Vashenko E., Selivanov V., Potashnikov A., Vlasuyk I., Streeter L*. Analysis of current video databases for quality assessment // T-Comm. 2022. Т. 16. № 2. С. 48-56.
17. *Можаева А.И., Власюк И.В., Поташников А.М., Стритер Ли*. Эталонная объективная метрика оценки качества видео совместимая с PSNR учитывающая частотные и периферическую характеристики зрения человека // DSPA: Вопросы применения цифровой обработки сигналов. 2021. Т. 11. № 2. С. 44-54.
18. *Valitskaya N.S., Vlasyuk I.V., Potashnikov A.M.* Video compression method on the basis of discrete wavelet transform for application in video information systems with non-standard parameters // T-Comm. 2020. Т. 14. № 3. С. 47-53.
19. *Поташников А.М., Власюк И.В*. Метод построения равноконтрастного цветового пространства для заданной системы отображения информации и условий контроля // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 15-22.

ВОЛОКОННО-ОПТИЧЕСКИЙ ДАТЧИК СИСТЕМЫ ОХРАНЫ ПЕРИМЕТРА ОБЪЕКТА

Мансуров Тофиг Магомед оглы,
Азербайджанский Технический Университет, профессор, д.т.н., Баку, Азербайджан
tofiq-mansurov@rambler.ru

Мамедов Рахман Салман оглы,
Азербайджанский Технический Университет, доцент, к.т.н., Баку, Азербайджан

Мансуров Эльнур Тофиг оглы,
Азербайджанский Технический Университет, докторант, Баку, Азербайджан

Аннотация

Проведен анализ существующих волоконно-оптических датчиков системы обнаружения несанкционированного проникновения на территорию охраняемого объекта. Отмечено, что привлекательной особенностью таких датчиков является невосприимчивость к электромагнитным излучениям и электробезопасность. В результате проведенного анализа сделан вывод о том, что известные волоконно-оптические датчики в отдельности позволяют выявить только факт несанкционированного проникновения, а при многозонной охранной системы - и факта, и зоны несанкционированного проникновения, но не причину срабатывания волоконно-оптического датчика, т.е. параметра объекта-нарушителя (мелкое животное, человек или транспортное средство). Для расширения функциональной возможности разработан волоконно-оптический датчик, позволяющий определить не только факт проникновения, но и параметры объекта-нарушителя, а именно его массу. Выбрано оптическое волокно для разрабатываемого волоконно-оптического датчика и формирователя макроизгиба оптического волокна с наибольшей восприимчивостью к макроизгибу - G 655. Установлено, что увеличение длины дуги макроизгиба при постоянном радиусе формирователя макроизгиба приводит к возрастанию затухания сигнала оптического излучения в оптическом волокне. Указано, что эта зависимость близка к линейной в диапазоне длин дуги макроизгиба от нуля до πR.

Ключевые слова: *Оптическое волокно, датчик, чувствительный элемент, охраняемый объект, макроизгиб, деформация, вибрация, коэффициент затухания, масса*

Введение

В волоконно-оптических датчиках в качестве чувствительного элемента детектирования изменения информационных параметров о состоянии того или иного охраняемого объекта в основном используется оптическое волокно и является пассивным компонентом волоконно-оптической линии связи, что расширяет области их применения. В настоящее время разработаны множество волоконно-оптических датчиков, позволяющее регистрировать деформацию, вибрацию, угол наклона, ускорения, перемещения, давление, а также обнаруживать несанкционированное проникновение на территорию охраняемого объекта [2-10].

Для измерения вибраций, деформаций и др. механических воздействий в качестве волоконно-оптических датчиков системы охраны периметра объекта могут применяться оптические волокна, по которым одновременно передается полезная информация. Такие датчики применяются в оптических системах безопасности в целях разработки сигнальных систем для охраны периметра объектов. Применяемость волоконно-оптических технологий определяется в основном с невосприимчивостью к электромагнитным полям и электрической безопасностью.

При проникновении на территорию охраняемого объекта создается внешние воздействия в виде механических давлений, деформаций и/или вибраций, которые в свою очередь, приводит к изменению параметров среды передачи и, как следствие, параметров переданного через оптическое волокно сигнала оптического излучения.

Постановка задачи

В настоящее время известны волоконно-оптические датчики [2-10], позволяющие обнаруживать только факт несанкционированного проникновения на территорию охраняемого объекта, не может определить причину срабатывания волоконно-оптического датчика, например, человек, мелкое животное, транспортное средство и т.д.

В связи с этим возникает задача разработки волоконно-оптического датчика системы охраны периметра объекта, позволяющий определить не только сам факт проникновения, но и параметры, а именно массу проникающих объектов (нарушителя).

Для разработки волоконно-оптического датчика выбрано оптического волокна типа G 655 с наибольшей восприимчивостью к макроизгибу. Установлено, что увеличение длины дуги макроизгиба при постоянном радиусе приводит к возрастанию затухания сигнала оптического излучения в оптическом волокне.

Целью данной работы является разработка волоконно-оптического датчика системы охраны периметра объекта, который позволил бы определить не только сам факт проникновения, но и параметры проникающего объекта (нарушителя), а именно массу.

Для решения поставленной задачи проведена классификация существующих волоконно-оптических датчиков, указаны преимущества и особенности.

Теперь рассмотрим их в отдельности.

Основные виды волоконно-оптических датчиков

Волоконно-оптические датчики с применением оптического волокна можно разделить на датчики, в которых оптическое волокно используется в качестве среды передачи, и датчики, в которых оптическое волокно используется в качестве чувствительного элемента от механических проникновений.

Существующие волоконно-оптические датчики подразделяется на две группы, т.е. активные и пассивные датчики [2].

Принцип работы активных датчиков заключается в том, что при воздействии на них измеряемой величины они сами генерируют сигнал оптического излучения, который по второму оптическому волокну поступает на фотоприемник. В этом случае информационным параметром генерируемого сигнала оптического излучения является его интенсивность, т.е. оптическая мощность.

В пассивных датчиках измеряемая величина сама модулирует проходящий через него сигнал оптического излучения, генерируемого источником оптического излучения.

Наряду с этими существуют точечные и распределенные датчики различных величин.

Точечные датчики разделяются на датчики вибрации, деформации, давления, температуры, угла наклона и линейных перемещений.

Распределенные датчики разделяются на датчики температуры и деформации.

Основные достоинства волоконно-оптических датчиков

В известных работах [2-10] показана возможность создания волоконно-оптических датчиков на основе макроизгиба оптического волокна.

Волоконно-оптические датчики на основе оптического волокна имеет возможности мультиплексирования, стабильности, проведения дистанционного измерения, устойчивы к влиянию электромагнитных полей, отсутствует электричества в точке проведения измерения.

К основным достоинствам таких волоконно-оптических датчиков по сравнению с электрическими датчиками можно отнести электрическую безопасность, невосприимчивость к электромагнитным полям и возможность использования в сочетании с теми оптическими волокнами, по которым осуществляется передача необходимой информации о состоянии охраняемого объекта. Последнее позволяет избегать преобразования электрического сигнала в оптический и упростить системы диагностики состояния объектов.

Особенности волоконно-оптических датчиков

К основным особенностям волоконно-оптических датчиков относится [3,5]:

- отсутствие вдоль охраняемого периметра электромагнитного излучения от волоконно-оптических датчиков (нет активного оборудования на периметре охраняемого объекта), поэтому затруднена или

полностью отсутствует возможность обнаружения трассу, по которой размещены волоконно-оптические датчики - кабеля, он полностью взрыво- и пожаробезопасен;

- имение возможности охраны сложных и протяженных периметров объектов;
- неимение чувствительности волоконно-оптического датчика к внешним электромагнитным полям, излучениям и наводкам;
- имение возможности использовать в качестве волоконно-оптического датчика стандартных типов оптических волокон;
- имение возможности использовать в качестве волоконно-оптического датчика одну из оптических волокон уже проложенного волоконно-оптического кабеля;
- имение возможность интеграции с системами охраны периметра объекта более высокого уровня иерархии;
- имение интерфейса на рабочем месте оператора системы охраны периметра объекта;
- имение возможности разграничения уровня доступа персонала, работающего с системой охраны периметра объекта;
- ведение журнала наблюдений за состоянием периметра охраняемого объекта с возможностью просмотра и включения фильтров различения по видам событий;
- имение возможности оповещения системы охраны периметра объекта о возникшей внештатной ситуации по SMS и/или по e-mail;
- имение возможности привязки границ периметра охраняемого объекта к реальным географическим координатам с помощью GPS;
- обучаемый комплекс алгоритмов распознавания событий / попыток нарушения периметра охраняемого объекта;
- возможность организации удаленного доступа к программной части охранной системы периметра объекта;
- встроенные элементы для проведения самодиагностики состояния волоконно-оптического датчика;
- аппаратные средства самодиагностики процесса функционирования программной части системы охраны периметра объекта;
- в случае программного сбоя автоматическое восстановление функционирования системы охраны в течение 60 сек.;
- защита доступа к программной части волоконно-оптической системы охраны периметра объекта ключом шифрования.

Разработка волоконно-оптического датчика и формирователя макроизгиба

На основе проведенного анализа разработана обобщенная схема волоконно-оптического датчика, которая представлена на рисунке 1.

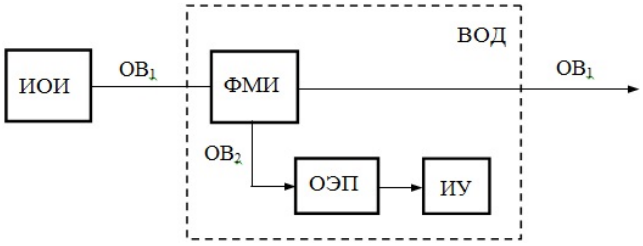

Рис. 1. Обобщенная схема волоконно-оптического датчика

Волоконно-оптический датчик содержит источник оптического излучения (ИОИ), формирователя макроизгиба (ФМИ), оптоэлектронного преобразователя (ОЭП), состоящего из фотодетектора и усилителя, и измерительного устройства. ИОИ формирует сигнал оптического излучения с определенной длиной волны и передает по первому оптическому волокну ($ОВ_1$). ФМИ создает макроизгиб с различными диаметрами и в соответствии с этим происходит ответвление сигнала оптического излучения, интенсивность которого зависит от диаметра макроизгиба и ответвленного сигнала оптического излучения передается по второму оптическому волокну ($ОВ_2$). ОЭП преобразует ответвленный сигнал оптического излучения в электрический сигнал и усиливает.

Ответвление части интенсивности переданного сигнала оптического излучения из первого оптического волокна можно осуществить с помощью формирователя макроизгиба, который в основном подключается к первому оптическому волокну, по которому передается полезная информация. Подключение данного формирователя осуществляется с целью идентификации оптического волокна передачи полезной информации и при необходимости организации кратковременной служебной линии связи для операторов. Необходимо отметить, что формирователи макроизгиба используются для несанкционированного съема информации [2, 3, 9, 10].

Разработаны волоконно-оптический датчик с формирователем макроизгиба (ФМИ) оптического волокна и измерительное устройство (УБ), схемы которых представлены на рисунках 2 и 3 [1].

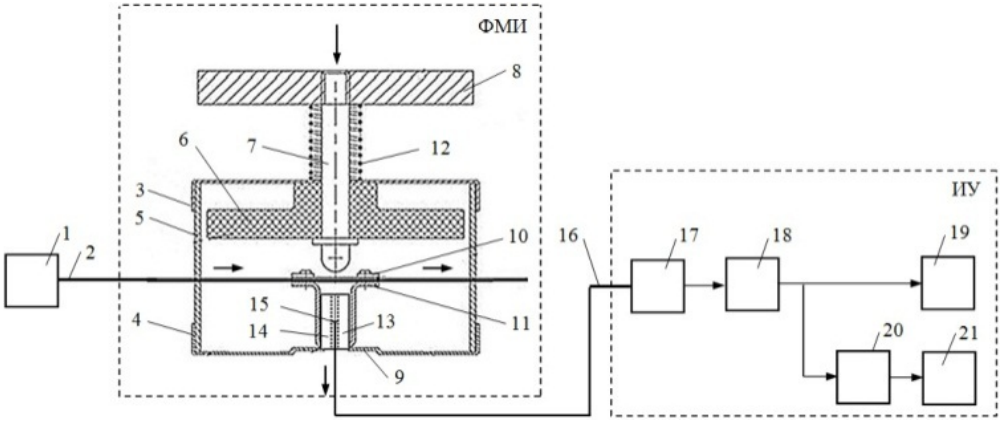

Рис. 2. Схема волоконно-оптического датчика

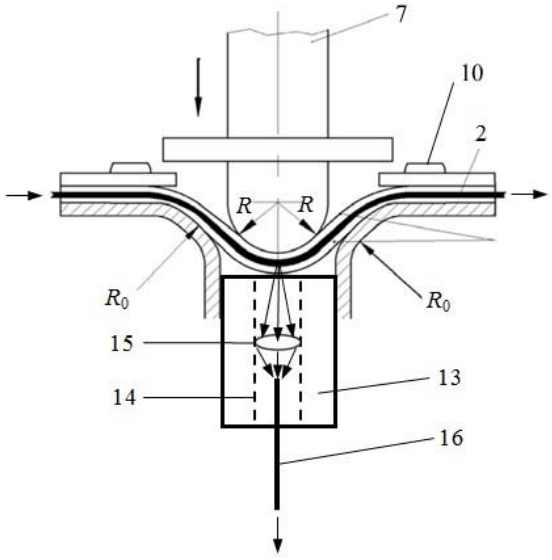

Рис. 3. Схема формирователя макроизгиба оптического волокна

Функциональные узлы волоконно-оптического датчика

Волоконно-оптический датчик системы охраны периметра объекта состоит из источника оптического излучения -1, первого оптического волокна -2 с сердцевиной и светоотражающим покрытием, верхней -3 и нижней крышки -4, кожуха -5, направляющей -6, подвижного стержня -7, кнопки -8, опоры -9, планки -10, мембран -11, пружины -12, неподвижного стержня -13, отверстии в виде воронки -14, линзы -15, размещенной в отверстии в виде воронки -14 и напротив участка с макроизгибом, второе оптическое волокно -16 с сердцевиной и светоотражающим покрытием для передачи ответвленного сигнала оптического излучения, фотодетектора -17, усилителя -18, измерителя уровня -19, электронного отчетного устройства -20, выполняющего математические операции и электронного индикатора -21 (см. рис. 2 и 3) [1].

Принцип работы волоконно-оптического датчика

Волоконно-оптический датчик работает следующим образом [1].

В процессе несанкционированного проникновения в охраняемый объект при нажатии кнопки -8 телом с массой *m* подвижный стержень -7 перемещается вниз по направляющей -6 и прижимается к мембранам -11. Между мембранами уложено оптическое волокно. Для предотвращения соскальзывания первого оптического волокна -2 в стороны при сжатии и создании макроизгиба в виде дуги окружности в одной из мембран -11 размещены два невысокие параллельные направляющие ролики. Оптическое волокно -2 располагается между этими роликами. Такое расположение предотвращает скольжение оптического волокна -2 в сторону в случае воздействия на мембрану -11 подвижного стержня -7, а при прекращении воздействия способствует распрямлению оптического волокна. При прекращении воздействия на кнопку -8 телом с массой *m* -8 пружина -12 раскрывается, подвижный стержень -7 возвращается в исходное положение, а первое оптическое волокно -2 возвращается в прямолинейное положение.

В результате воздействия подвижного стержня -7 на мембраны -11 происходит процесс макроизгиба первого оптического волокна -2, радиус которого соответствует радиусу *R* круглого конца подвижного стержня -7 (см. рис. 3). С помощью круглого конца подвижного стержня -7 формируется макроизгиб первого оптического волокна -2 с соответствующим радиусом *R* и от этого макроизгиба происходит ответвление оптического излучения, которое проходит через отверстии в виде воронки -14, линзу -15, размещенная в отверстии в виде воронки, напротив участка с макроизгибом и данное излучение с помощью линзы фокусируется на вход второго оптического волокна -17, вход которого размещен в точке фокуса линзы -15. С выхода второго оптического волокна -17 попадает на вход фотоприемника -16, преобразующего ответвленного оптического излучения в электрический сигнал, с выхода фотоприемника на вход усилителя -18, с выхода усилителя параллельно на вход измерителя уровня -19 и электронного отчетного устройства -20, автоматически выполняющего математические операции, с выхода электронного отчетного устройства -20 на вход электронного индикатора -21.

Первое оптическое волокно -2 вместе с мембранами -11 крепится к опорам -9, а расстояние между ними равно диаметру подвижного стержня -7. Края опор -9 выполнены в виде круглой воронки с радиусом *R*, что позволяет исключить ослабление при макроизгибе ответвленного оптического излучения на краях опор -9 (см. рис. 3).

Подвижный стержень -7 опирается на плечи опор -9, для ограничения ее перемещения используется опора -9, что предотвращает разрыв мембран -11 и первого оптического волокна -2 при возникновении сильного удара.

При воздействии на кнопку -8 волоконно-оптического датчика какой-либо массой происходит процесс ответвления оптического излучения, передаваемого источником оптического излучения -1 по первому оптическому волокну, которое проходя через линзу -15, размещенной в отверстии в виде воронки, напротив участка с изгибом и второе оптическое волокно -16 параллельно поступает на вход измерителя уровня -19 и электронного отчетного устройства -20. Измеритель уровня -19 измеряет Δa – затуханию ответвленного оптического излучения.

С другой стороны, зависимость между затуханием Δa и массой m определяется следующим выражением:

$$\Delta a = (mg)/k, \tag{1}$$

где m – масса, действующая на кнопку волоконно-оптического датчика; g – ускорение свободного падения; k – коэффициент жесткости пружины.

Используя выражение (1), зависимости между массой m, действующей на кнопку волоконно-оптического датчика и создаваемым при этом ослаблением Δa, можно определить следующим образом:

$$m = (\Delta a \cdot k)/g. \tag{2}$$

После того, как значение изменения затухания Δa известно, на выходе электронного отчетного устройства -20, выполняющее математические операции по выражению (2), получается значение физической величины, пропорциональной проникающей массе m, которое передается на вход электронного индикатора -21, шкала которого откалибрована пропорционально массе m. На шкале электронного индикатора получается значение, пропорциональное массе, что позволяет определить массу m, осуществляющей несанкционированное проникновение на охраняемую территорию объекта.

Таким образом, введение в предлагаемый волоконно-оптический датчик источника оптического излучения, неподвижного стержня с отверстием в виде воронки, линзы, размещенной в этом отверстии, напротив участка с изгибом, второго оптического волокна, обеспечивающего передачи ответвленного сигнала оптического излучения, фотоприемника, усилителя, измерителя уровня, электронного отчетного устройства, автоматически выполняющего математические операции, электронного индикатора, в зависимости от интенсивности ответвленного сигнала оптического излучения позволяет обнаружить несанкционированное проникновение на охраняемую территорию объекта, увеличение диапазона измерения за счет усиления ответвленного сигнала оптического излучения, подбор коэффициента жесткости пружины увеличивает предел измерения массы тела объекта при несанкционированном проникновении и тем самым расширить его функциональные возможности.

Заключение

Таким образом, в зависимости от интенсивности ответвленного сигнала оптического излучения, разработанный волоконно-оптический датчик системы охраны периметра объекта позволяет обнаружить несанкционированное проникновение на охраняемую территорию объекта, увеличить диапазон измерения затухание ответвленного сигнала оптического излучения за счет его усиления, правильно выбрать коэффициента жесткости пружины для увеличения предела измерения массы тела объекта несанкционированного проникновения. Обеспечение этих критерий позволяет расширить его функциональные возможности.

На основе проведенных экспериментальных исследований сделан вывод о том, что меньше 50% интенсивности источника оптического излучения получается на выходе волоконно-оптического датчика и передается по первому оптическому волокну, а больше 50% на прямом выходе первого оптического волокна.

Если уровень выходной интенсивности источника оптического излучения, передаваемого по первому оптическому волокну равна 0 дБм (1,0 мВт), и к.п.д. волоконно-оптического датчика около 5% (-13дБ), то потери на макроизгибе первого оптического волокна примерно составляет 1,0дБ. Это означает, что для создания оптического канала ответвления выходной мощности источника сигнала оптического излучения по второму оптическому волокну можно сформировать макроизгиб, имеющий диаметр 5,0…60 мм.

Литература

1. *Мансуров Т.М., Юсифбайли Н.А., Джебраилова С.А., Мансуров Э.Т.* Волоконно-оптический сенсор / Агентство интеллектуальной собственности Азербайджанской Республики. Номер приоритета заявки № a2022 0154. Баку, 2022. 8 с.

2. *Василевский Г.В., Зеневич А.О., Жданович С.В., Лукашик Т.М., Лагутик А.А.* Использование макроизгиба оптоволокна в качестве основы для создания датчика массы. Санкт-Петербург: СПбГУ ИТМО. Изв. вузов «Приборостроение», 2020. Т. 63, №10. С. 930-937.

3. *Гулаков И.Р., Зеневич А.О., Мансуров Т.М.* Компоненты волоконно-оптических линий связи. Учебное пособие. Минск, БГАС, 2020. 336 с.

4. *Ren L.* Design and experimental study on FBG hoop-strain sensor in pipeline monitoring // Optical fiber technology. 2014. Vol. 20. No. 1. P. 15-23.

5. *Li L.* Design of an enhanced sensitivity FBG strain sensor and application in highway bridge engineering // Photonic Sensors. 2014. Vol. 4. No. 2. P. 162-167.

6. *Бурдышева О.В., Шолгин Е.С.* Волоконно-оптический датчик вибрации // Специальный выпуск «Фотон-экспресс-наука 2019», 2019. № 6. С. 52-53.

7. *Chen W.* et al. Performance assessment of FBG temperature sensors for laser ablation of tumors // IEEE Intern. Symp. on Medical Measurements and Applications (MeMeA). 2015. P. 324-328.

8. *Mamidi V.R.* et al. Fiber Bragg Grating-based high temperature sensor and its low cost interrogation system with enhanced resolution // Optica Applicata. 2014. Vol. 44, № 2. P. 299-308.

9. *Куликов А.В., Игнатьев А.В.* Обзор волоконно-оптических систем охраны периметра // Алгоритмы безопасности. Санкт-Петербург, 2010. № 4. С. 56-61.

10. *Василевский Г.В., Зеневич А.О., Лагутик А.А, Лукашик Т.М., Новиков Е.В.* Исследование характеристик отраженного излучения в оптическом волокне как основы для создания волоконно-оптических датчиков // Зв'язок. 2019. № 1. С. 40-44.

КВАЛИМЕТРИЧЕСКИЙ КОНТРОЛЬ КРИТИЧЕСКОЙ НАДЕЖНОСТИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДИЧЕСКИХ И МАТЕМАТИЧЕСКИХ ИНСТРУМЕНТОВ ТЕОРИИ КАТАСТРОФ

Паращук Игорь Борисович,
Военная академия связи им. Маршала Советского Союза С.М. Буденного, профессор кафедры автоматизированных систем, д.т.н., профессор, Санкт-Петербург, Россия
shchuk@rambler.ru

Михайличенко Антон Валерьевич,
Военная академия связи им. Маршала Советского Союза С.М. Буденного, адъюнкт кафедры автоматизированных систем, Санкт-Петербург, Россия
toni09_91@mail.ru

Смирнов Александр Андреевич,
Военная академия связи им. Маршала Советского Союза С.М. Буденного, соискатель кафедры автоматизированных систем, Санкт-Петербург, Россия
alexsmirrrrn@yandex.ru

Аннотация
В статье описан методологический подход, нацеленных на реализацию математически корректных процедур выявления и распознавания граничных и предаварийных (катастрофичных) значений критической надежности центров обработки данных при плавных изменениях параметров внешних условий и управляющих воздействий, влияющих на их безотказность, ремонтопригодность, восстанавливаемость и сохраняемость. Подход использует методические и математические инструменты теории катастроф и позволяет не допустить аварийного (катастрофичного) скачкообразного изменения надежности системы при малых возмущениях.

Ключевые слова: *теория катастроф, центр обработки данных, надежность, аппаратные и программные средства*

Введение

Результаты детального анализа итогов современных научных и практических исследований, посвященных вопросам текущего контроля и прогнозирования качества функционирования аппаратных и программных средств, составляющих основу сложных управляемых технических систем, например, таких, как центры обработки данных (ЦОД) или, иначе, дата-центры, предопределяют объективную важность, первоочередность формулировки концепции и создания методов и моделей квалиметрии критической надежности – одной из важнейших составляющих устойчивости, а, в конечном итоге, важной составляющей качества систем такого класса [1-4].

При этом под квалиметрией критической надежности понимается оценка (определение) кризисных запасов по качеству (с точки зрения технической надежности), т.е. оценка критических величин параметров надежности (безотказности, ремонтопригодности, восстанавливаемости и сохраняемости), приводящих к рискам потери качества объекта – отказу, сбою аппаратных или ошибкам программных средств центров обработки данных [5].

Критические величины параметров надежности (безотказности, ремонтопригодности, восстанавливаемости и сохраняемости) ЦОД могут быть достигнуты в ходе эксплуатации систем такого класса, зачастую, незаметно для обслуживающего персонала, постепенно нарастая до граничных, зачастую катастрофических значений, вызывая лавинообразный сбой (коллапс, отказ) системы.

Современным ЦОД в условиях нынешнего бурного развития единого информационного пространства и совершенствования процессов автоматизации управления в различных сферах человеческой деятельности, принадлежит весьма важная, а в ряде случаев, и ключевая роль.

Даже кратковременное нарушение надежного функционирования аппаратных и программных средств ЦОД, может привести к непредсказуемым, а иногда и катастрофическим последствиям для

информационного обеспечения и автоматизации управления объектами инфраструктуры и жизнеобеспечения. Все это обуславливает актуальность научной задачи объективной и многокритериальной оценки критической надежности программных и технических элементов (например, микропроцессорных подсистем и цифровых подсистем хранения данных) ЦОД, а также оценки надежности систем такого класса в целом.

Не секрет, что надежность аппаратного или программного элемента ЦОД – его способность сохранить устойчивость процесса функционирования этого конкретного элемента, заключающуюся в отсутствии вынужденных прекращений этого процесса (срывов, отказов, сбоев функционирования – для аппаратных средств) и неправильных действий (ошибок – для программных средств) [4].

Что касается устойчивости, то данное свойство аппаратных и программных элементов ЦОД характеризует их способность достигать целей своего функционирования в условиях всех видов позитивных и негативных воздействий и оценивается, опираясь на параметры живучести, помехоустойчивости и технической надежности как самих элементов, так и ЦОД в целом. Оценка надежности (как составляющей устойчивости) аппаратных и программных средств, как правило, проводится на трех ключевых уровнях: объектовом, структурном и функциональном [3-5].

Анализ показывает, что аппаратные и программные средства (элементы) современных ЦОД не в полной мере удовлетворяют требованиям по надежности, в частности, с точки зрения медленного и монотонного характера изменения наружных и внутренних параметров среды и самой ЦОД в ответ на плавный дрейф этих параметров в процессе функционирования дата-центра.

Именно поэтому перспективным, на наш взгляд, направлением совершенствования методологии оценки (определения) критической надежности аппаратных и программных средств ЦОД, является разработка алгоритмов анализа безотказности, ремонтопригодности, восстанавливаемости и сохраняемости элементов дата-центров на основе применения методических и математических инструментов теории катастроф, с учетом динамики возможного скачкообразного изменения значений параметров надежности элементов ЦОД в ответ на медленное и монотонное изменение характера и глубины наружного или внутреннего воздействия. Данные алгоритмы, по нашему мнению, позволят производить достоверный и оперативный контроль критической надежности, осуществлять адекватную сравнительную многокритериальную оценку надежности элементов ЦОД и дата-центров в целом в интересах синтеза робастных алгоритмов динамического управления объектами такого класса.

Результаты исследований

Теория катастроф описывает скачкообразные изменения, возникающие в виде резкого, неожиданного и непредсказуемого, чаще – негативного, ответа системы на медленное и монотонное изменение наружных (окружающих внешних) условий и внутренних параметров среды и самой ЦОД. Методические и математические инструменты данной теории основаны на корректном аналитическом аппарате бифуркаций («складок», «сборок» и др.) и «особенностей», лежащем на стыке решения топологических и нетипичных вычислительных задач [6-8].

Методические и математические инструменты теории катастроф представляют собой набор используемых на практике методов и алгоритмов в рамках данной теории, они призваны аналитически описать и помочь лицам, принимающим решения, анализировать мгновенно и скачкообразно изменяющиеся состояние систем (в нашем случае – скачкообразное изменение значений показателей надежности ЦОД) при медленно, плавно и монотонно нарастающих воздействиях. С этой точки зрения термин «катастрофа» означает резкое качественное изменение (чаще всего – в отрицательную сторону) надежности элементов ЦОД и дата-центров в целом при плавном количественном изменении параметров безотказности, ремонтопригодности, восстанавливаемости и сохраняемости, из которых эта надежность состоит и от которых напрямую зависит [6, 8-11].

Иными словами, методические и математические инструменты теории катастроф позволяют анализировать скачкообразный переход количественной меры надежности в качественную, исследовать некие критические точки (точки Зимана-Морса) после достижения которых, в системе наступают непоправимые, безвозвратные изменения надежности.

Методические и математические инструменты теории катастроф, на наш взгляд, могут быть эффективно применены с целью решения подобных задач при анализе перспектив гарантированной надежной эксплуатации и в динамике работы реальных ЦОД, когда, скажем, показатель надежности, характеризующий, например, безотказность – коэффициент плотности (концентрации) аппаратных сбоев и

программных ошибок элементов $\rho^{э}_{псо}(t)$ дата-центра, может медленно и монотонно меняться под влиянием управляющих воздействий (допустим, снижения интенсивности технического обслуживания и ремонта) или внешних, природных или иных факторов (к примеру, нарастания отрицательных температур в среде применения), создавая потенциальную угрозу потери работоспособности, блокировки (коллапса) процесса функционирования для информационно-поисковых и вычислительных систем такого класса.

Применение методических и математических инструментов теории катастроф обеспечит способность выявления и распознавания предельных, пограничных и, возможно, предаварийных (экстремальных) состояний по надежности, в нашем случае, характерных для критических значений коэффициента плотности (концентрации) аппаратных сбоев и программных ошибок элементов $\rho^{э}_{псо}(t)$ ЦОД, когда имеются медленные и монотонные незначительные изменения наружных и внутренних параметров среды, самой ЦОД и управляющих воздействий на него. В конечном итоге, это позволит осуществлять выявление, распознавание и проактивное (упреждающее) оповещение администратора ЦОД об предаварийных условиях реализации процедур обмена и обработки данных, с точки зрения технической надежности объекта такого класса.

Это позволит надежно, устойчиво, своевременно и динамично осуществлять обмен и обработку данных на ЦОД в реальных условиях, когда есть угроза достижения критической (на границе возможностей реализации надежной эксплуатации), например, плотности (концентрации в единицу времени) аппаратных сбоев и программных ошибок (АСиПО) элементов ЦОД при плавных изменениях параметров внешних условий и управляющих воздействий.

Объективная возможность и уместность такого подхода обусловлены тем, что подобное положение дел способно проявится не сразу в ходе очередного этапа эксплуатации ЦОД, однако медленный и монотонный рост плотности (концентрации) аппаратных сбоев и программных ошибок элементов $\rho^{э}_{псо}(t)$ ЦОД, в вопросах прогноза и поддержания надежности дата-центра (при плавных и небольших изменениях параметров потока АСиПО), чреват катаклизмом, может грозить катастрофой. Именно поэтому, на наш взгляд, методические и математические инструменты теории катастроф могут реально помочь при контроле скачкообразных изменений критической надежности управляемого и анализируемого объекта – ЦОД, возникающих в виде внезапного ответа этой системы (объекта) на медленное и монотонное изменение параметров, вызванное управляющими или иными воздействиями.

Катастрофы (с точки зрения критической надежности) на ЦОД, приводят к частичной или полной блокировке реализуемых на них процессов, могут проявляться в форме спонтанных «лавинных» аппаратных сбоев и программных ошибок, поломок коммутационных устройств и устройств хранения и обработки данных, резких перепадов интенсивности нарушений производительности, а значит – скачкообразного изменения параметров безотказности, ремонтопригодности, восстанавливаемости и сохраняемости и т.п. Например, реализации процесса эффективной обработки данных в ЦОД, администратор этого дата-центра формирует команды управления, рассчитанные на определенную потенциальную надежность каналов межмашинного обмена, обеспечивающих необходимую пропускную способность системы поиска и обработки данных, учитывая допустимую плотность (вероятную концентрацию в единицу времени) АСиПО этих элементов – каналов. Вместе с тем, во время эксплуатации ЦОД происходит «монотонный дрейф» параметров потока АСиПО (связанное, например, с плавным снижением интенсивности технического обслуживания, ремонта и восстановления этих каналов), который в определенный момент времени готов и может привести к скачкообразному деструктивному изменению, резкому росту интенсивности отказов элементов, и, в конечном итоге, к потере надежности ЦОД.

Поэтому эффективная реализация процедур поиска и обработки данных на ЦОД должна быть ориентирована на безусловные выявление и распознавание предельных, пограничных и, возможно, предаварийных (экстремальных) состояний потока (значений коэффициента плотности) АСиПО элементов $\rho^{э}_{псо}(t)$ ЦОД.

Эти процедуры должны помочь предсказать возможное катастрофическое состояние самой системы, давая, тем самым, администратору ЦОД возможность избегнуть таких ненадежных состояний, характерных для предаварийного, почти критического состояния вектора параметров надежности (включающего параметры безотказности, ремонтопригодности, восстанавливаемости и сохраняемости) дата-центра.

При этом под «состоянием пограничного, предаварийного значения коэффициента плотности аппаратных сбоев и программных ошибок» элементов дата-центра

$$\rho^{э}_{\text{псо}}(t) = (\omega / t) \tag{1}$$

понимается количество (концентрация) ω зафиксированных за интервал времени t независимых либо зависимых друг от друга АСиПО.

Число ω зарегистрированных за интервал времени t АСиПО способно, медленно и монотонно нарастая до критической, кризисной цифры, в непредвиденный момент времени привести к резкому (в подавляющем большинстве случаев – негативному) изменению состояния этого показателя безотказности, к потере надежности ЦОД в целом, способно вызвать лавинообразное снижение надежности, а значит, и ухудшение итогового качества работы дата-центра, вплоть до блокирования его работы.

Таким образом, в рамках рассмотренного примера решается задача проактивного (упреждающего) оценивания и сравнения реальных и критических значений коэффициента плотности (концентрации) аппаратных сбоев и программных ошибок элементов ЦОД на основе методических и математических инструментов теории катастроф. По сути, это процесс априорного статистического анализа медленных и монотонных незначительных изменений параметров среды и условий эксплуатации ЦОД с возможностью оповещения (предупреждения) администратора о возможных потенциально катастрофических последствиях при потере его надежности.

При данном подходе к квалиметрическому контролю критической надежности аппаратных и программных средств центров обработки данных, есть возможность корректного аналитического описания динамики изменения состояния показателей надежности элементов данной системы при медленных и монотонных вариациях внешних условий и управляющих воздействий. Это описание можно осуществить в виде динамики изменения коэффициента плотности (концентрации) АСиПО элементов ЦОД (1), подлежащих анализу – изменения количества ω зафиксированных АСиПО элементов дата-центра за интервал времени t, обуславливаемый и задаваемый процедурами управления.

Анализ результатов работ [6-11] позволяет именно так описать и математически корректно реализовать возможность выявления и распознавания предельных, пограничных и предаварийных (экстремальных) состояний по надежности системы такого класса при медленных и монотонных «сдвигах» значений параметров внешних условий среды и управляющих воздействий.

Математическая формализация физических параметров этих условий и воздействий, влияющих на критическую надежность аппаратных и программных средств ЦОД, может быть представлена как статистика соответствующих значений коэффициента плотности аппаратных сбоев и программных ошибок $\rho^{э}_{\text{псо}}(t)$, как количества ω зафиксированных АСиПО за первый (стартовый) t и последующие ((t+1), … , (t+g), … , (t+(G–1)) интервалы времени наблюдения.

При этом коэффициент плотности аппаратных сбоев и программных ошибок элементов ЦОД $\rho^{э}_{\text{псо}}(t)$=1, 2, … , Λ может составлять, например, от одного до десяти тысячи, а количество g, где g = 1, 2, … , G – число следующих друг за другом временных интервалов t наблюдения в рамках рассмотренного примера, может быть от одного до тысячи.

Общее количество таких значений коэффициента плотности аппаратных сбоев и программных ошибок элементов ЦОД за все время наблюдения (время контроля критической надежности) равно Λ, причем данные значения можно записать в виде множества:

$$\begin{gathered}\Lambda_G = \{\rho^{э}_{\text{псо}\,1}(t), \rho^{э}_{\text{псо}\,2}(t+1), \ldots, \rho^{э}_{\text{псо}\,g}(t+g), \ldots \\ \ldots, \Lambda_G(t+(G-1))\},\end{gathered} \tag{2}$$

где любой g-ый элемент этого множества, кроме Λ_G (t+(G–1)), является подмножеством Λ_G и имеет физический смысл, заключающийся в том, что на интервале времени t критический порог надежности аппаратного или программного средства ЦОД по плотности потока АСиПО выше требуемого. А это значит, что высока вероятность перехода данного средства, элемента дата-центра, в аварийное, предельное (экстремальное) состояние по надежности на очередном временном интервале (t+1) наблюдения.

В этой связи предполагается очевидным, что для решения задачи проактивного (упреждающего) оценивания и сравнения значений плотности аппаратных сбоев и программных ошибок элементов ЦОД при медленных и монотонных изменениях параметров воздействий, требуется проводить текущий пошаговый мониторинг надежности, осуществлять выявление и распознавание предельных, пограничных и, возможно, предаварийных состояний системы с точки зрения ее безотказности, ремонтопригодности, восстанавливаемости и сохраняемости.

С использованием методических и математических инструментов теории катастроф выявление и распознавание пограничных и предаварийных состояний показателей надежности ЦОД производится

путем пошагового (на каждом шаге, т.е., каждом *g*-ом временном интервале (*t*+*g*) наблюдения) статистического расчета и сравнения значений каждого $\rho^{э}_{\text{псо}\,g}$ *g*-го элемента множества Λ_g с целью определения возможного превышения этими значениями допустимого порога (точки Зимана-Морса) концентрации или плотности потока АСиПО элементов ЦОД, описываемого уравнением:

$$\rho^{э}_{\text{псо}\,g}(t+g) \gtrless \Lambda_G, \tag{3}$$

где Λ_G – допустимое значение коэффициента плотности (концентрации) аппаратных сбоев и программных ошибок элементов ЦОД на *g*-ом отрезке времени контроля критической надежности $(t+g)$, при превышении которого аппаратный или программный элемент дата-центра с вероятнее всего перейдет в аварийное состояние с точки зрения надежности.

В пределах первого шага наблюдения, в раках начального, стартового временного интервала контроля критической надежности, это уравнение примет вид:

$$\rho^{э}_{\text{псо}\,1}(t) \gtrless \Lambda_1. \tag{4}$$

Если на одном из последующих ((*t*+1), (*t*+2) и т.д.) интервалов контроля критический порог надежности аппаратного или программного средства ЦОД по плотности потока АСиПО выше требуемого, это означает начало процесса «дрейфа параметра» – медленного и монотонного влияния изменения параметров внешних условий и управляющих воздействий на надежность.

Распознавание и подтверждение тенденции нарастания перспектив возникновения предельных, пограничных и, возможно, предаварийных (экстремальных) состояний потока АСиПО элементов ЦОД характеризует факт превышения любым значением коэффициента плотности аппаратных сбоев и программных ошибок $\rho^{э}_{\text{псо}\,g}$ элементов ЦОД на предыдущем временном интервале *t* контроля критической надежности (отсчета параметра потока АСиПО $(\rho^{э}_{\text{псо}\,1})$) над значением этого коэффициента с каждого следующего отсчета $(\rho^{э}_{\text{псо}\,2})$ на последующем временном интервале (*t*+1) контроля критической надежности. Данное значение определяется, например, для первого и второго временного интервала контроля критической надежности (интервала наблюдения) в соответствии с уравнением

$$\rho^{э}_{\text{псо}\,1}(t) \gtrless \rho^{э}_{\text{псо}\,2}(t+1). \tag{5}$$

Этим путем выявляется тенденция приближения значений параметров надежности (например, плотности аппаратных сбоев и программных ошибок) к рубежам предаварийного (возможно, катастрофичного) состояния элемента ЦОД с точки зрения надежности. При осуществлении процедуры выявления предаварийных значений этого показателя безотказности, когда идентифицировано событие

$$\rho^{э}_{\text{псо}\,g}(t+g) > \Lambda_g, \tag{6}$$

а также так и при осуществлении процедур распознавания, когда подтверждена тенденция изменения параметров надежности (например, плотности аппаратных сбоев и программных ошибок) в сторону предаварийного состояния элемента ЦОД с точки зрения надежности

$$\rho^{э}_{\text{псо}\,1}(t) < \rho^{э}_{\text{псо}\,2}(t+1), \tag{7}$$

администратор, отвечающий за управление процессом эксплуатации ЦОД, может и должен быть предупрежден о возможном аварийном состоянии системы с точки зрения достижения ею критической надежности [6].

Примеры, иллюстрирующие аналогичные, с точки зрения применения методических и математических инструментов теории катастроф, операции предотвращения потери устойчивости и анализа критической надежности сложных управляемых систем при плавных изменениях внешних условий, приведены в работах [12-15]. Здесь представлены алгоритмы анализа структурной надежности и устойчивости объектов, а также оценки критических точек (точек Зимана-Морса) в процессе функционирования системы, характеризующих локальные максимумы и минимумы надежного и устойчивого (не катастрофичного) поведения объекта при медленных, монотонных и незначительных изменениях

внешних условий.

Заключение

Рассмотренный подход может быть использован для решения задач многокритериальной оценки критической надежности программных и технических средств ЦОД, а также оценки и контроля критических значений параметров безотказности, ремонтопригодности, восстанавливаемости и сохраняемости систем такого класса в целом.

Предложен, по сути, основанный на применении методических и математических механизмов, т.е., методов и алгоритмов теории катастроф, квалиметрический подход к корректной реализации процедур выявления (идентификации), распознавания и подтверждения (верификации) предельных, пограничных и, возможно, предаварийных (экстремальных) состояний значений критической надежности ЦОД при медленных и монотонных изменениях параметров внешних условий и управляющих воздействий (например, плавных изменениях плотности потока АСиПО элементов ЦОД).

Данный подход позволяет повысить объективность формулировки адекватных процедур контроля надежности и связанных с ними алгоритмов управления центрами обработки данных, повысить надежность процедур обработки информации на дата-центре в реальных условиях, когда есть угроза достижения критических (на границе возможностей) значений показателей безотказности, ремонтопригодности, восстанавливаемости и сохраняемости ЦОД при плавных изменениях параметров внешних условий и управляющих воздействий.

Литература

1. *Докучаев В.А., Кальфа А.А., Маклачкова В.В*. Архитектура центров обработки данных. М.: Горячая линия – Телеком, 2020. 240 с.

2. *Крюкова Е.С., Ткаченко В.В., Михайличенко А.В., Паращук И.Б*. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 86-95.

3. *Лаврищева Е.М., Пакулин Н.В., Рыжов А.Г., Зеленов С.В*. Анализ методов оценки надежности оборудования и систем. Практика применения методов. Труды ИСП РАН, том 30, вып. 3, 2018. С. 99-120.

4. Межгосударственный стандарт ГОСТ 27.002-2015 Надежность в технике. Термины и определения. М.: Стандартинформ., 2016. 30 с.

5. Национальный стандарт РФ ГОСТ Р 51901.5-2005 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности. М.: Стандартинформ, 2005. 44 с.

6. *Арнольд В.И.* Теория катастроф. М.: Едиториал УРСС, 2004. 128 с.

7. *Павлова Н.Г., Ремизов А.О*. Введение в теорию особенностей. М.: Изд-во МФТИ, 2022. 181 с.

8. *Гилмор Р.* Прикладная теория катастроф. Книга 2. М.: Мир, 1984. 285 с.

9. *Poston T., Stewart I*. Catastrophe Theory and Its Applications. Dover Publications, Incorporated, 2013. 512 p.

10. *Петров Ю.П., Петров Л.Ю.* Неожиданное в математике и его связь с авариями и катастрофами последних лет. СПб.: НИИХ СПбГУ, 1999. 108 с.

11. *Седых В.Д.* Математические методы теории катастроф: учебное пособие. М.: Московский центр непрерывного математического образования. 2021. 224 с.

12. Паращук И.Б., Дьяков С.В. Математика теории катастроф применительно к задачам анализа надежности элементов сети связи / Системы связи. Анализ. Синтез. Управление / Под ред. проф. Постюшкова В.П. Выпуск 5. – СПб.: Изд-во «Тема», 2001. С. 47-49.

13. *Паращук И.Б.,* Чечулин А.А. Обеспечение безопасности беспилотных транспортных средств «умного города» с использованием проактивного поиска уязвимостей в человеко-машинных интерфейсах взаимодействия на основе методов теории катастроф // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г.: Материалы конференции. СПОИСУ. СПб: 2022. С. 116-118.

14. *Острейковский В.А., Саакян С.П., Силин Я.В*. Прогнозирование техногенного риска динамических систем методами теории катастроф // Фундаментальные исследования. 2012. № 3-2. С. 399-402.

15. *Гуц А.К., Лавров Д.Н.* Описание DDOS-атаки с помощью катастрофы «сборка» // Математические структуры и моделирование. 2013. № 1 (27). С. 42-45.

ПРОТИВОДЕЙСТВИЕ УТЕЧКАМ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЗ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Сиротский Алексей Александрович,
Национальный исследовательский Московский государственный строительный университет (НИУ МГСУ), доцент, к.т.н., Москва, Россия
hotwater2009@yandex.ru

Аннотация
В статье рассматриваются актуальные проблемы обеспечения безопасности персональных данных, обрабатываемых в информационно-телекоммуникационных системах и сетях. Проведённое исследование на основе моделирования с применением двудольного графа показало, что во многих случаях не обеспечивается принцип двойственности или парности построения рубежей безопасности. Также проведён анализ номенклатуры и видов программно-аппаратных решений, необходимых для создания систем защиты персональных данных и показаны трудности при проведении аналитического сопоставления функций безопасности различных защитных продуктов, что сильно осложняет квалифицированный подбор комплекса средств обеспечения безопасности. В работе предложено создание унифицированной системы формализованного представления функций безопасности и выделение наборов дискретных сопоставимых показателей, которые могут стать основой единой методологии интегративного метамоделирования взаимодействия программных комплексов защиты информации с информационными системами персональных данных.

Ключевые слова: *персональные данные, утечки, защита, сети, телекоммуникации, сетевая инфраструктура, цифровизация, системы, оборудование, моделирование, средства*

Введение

Вопросы обеспечения безопасности персональных данных за последние годы только повышают свою актуальность и могут рассматриваться в различных концептуальных проблемах делового оборота [1, 2, 3].

В России регулирование оборота персональных данных было установлено с 2006 года Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ. За свой период существования закон «О персональных данных» претерпевал изменения 28 раз. Впервые изменения произошли в 2009 году, а последние изменения состоялись в 2022 году, часть из которых уже вступила в силу [4], а часть вступит в силу с 1 марта 2023 года. Однако и сейчас уже назрели новые изменения, которые проходят стадии подготовки и обсуждений.

Причина такой высокой динамики законодательства о персональных данных заключается прежде всего в опережающих темпах развития информационно-телекоммуникационных технологий и активной цифровизации общественных и деловых процессов [5].

За последние десятилетия возникли и стали активно развиваться электронные услуги и сервисы, облачные технологии, электронные средства телекоммуникаций. Во всех этих средствах и системах обрабатываются огромные массивы информации, которые в настоящее время характеризуются термином «большие данные», в том числе содержащие персональные данные пользователей.

Если на первых порах наиболее актуальными были проблемы обеспечения защищённого доступа, защиты информации, данных и транзакций в финансово-кредитной сфере, находящейся на передовых позициях внедрения сервисов удалённого доступа [6, 7], то сегодня проблемы обеспечения безопасности сетевой инфраструктуры актуальны практически для всех предметных сфер деятельности.

Результаты исследований

Из открытых источников [8] известно, что только за 2022 год произошло несколько серьёзных утечек персональных данных из довольно крупных компаний (табл. 1).

Таблица 1

Сведения о крупных утечках персональных данных в 2022 году

Компания	Сфера деятельности	Количество записей	Содержание персональной информации
Яндекс.Еда	Доставка еды	50 млн	фамилия, номер телефона, адрес доставки
Delivery Club	Доставка еды	2 млн	имя, номер телефона, адрес доставки, адрес электронной почты, состав, стоимость, дата и время заказа, IP-адрес
Гемотест	Медицинские услуги	31 млн	дата рождения, адрес, номер телефона, адрес электронной почты, серия и номер паспорта, результаты анализов
СДЭК	Транспортная компания	466 млн и 822 млн	номер телефона, ФИО, адрес электронной почты, почтовый адрес
Почта России	Почтовая компания	10 млн	номер отслеживания посылки, ФИО (или название компании) отправителя и получателя, телефон получателя, город отправителя и получателя
Tutu.ru	Туристический сервис	2,2 млн	фамилия, номер телефона, адрес электронной почты
GeekBrains	Учебная он-лайн платформа	200 тыс	адрес электронной почты, номер телефона
Яндекс.Практикум	Учебная он-лайн платформа	300 тыс	имя, фамилия, имя пользователя, адрес электронной почты, номер телефона
РИА Новости	Информационное агентство	660 тыс	фамилия, логин, адрес электронной почты, профили социальных сетей
Pikabu	Развлекательный сайт	1 млн	адрес электронной почты, номер телефона
Метрополис	Торговый центр	80 тыс	адрес электронной почты, имя, количество бонусов, ссылки на социальные сети
Kari	Магазин обуви	1 млн	телефон, адрес электронной почты, дата рождения, город проживания, номер бонусной карты
Умный дом	Электронный сервис	700 тыс	адрес электронной почты, телефон, IP-адрес, дата регистрации и последней активности
Tele2	Оператор мобильной связи	7 млн	имя, номер телефона, адрес электронной почты

Как видно, общей характеристикой практически всех приведённых в табл. 1 компаний является их активная позиция по развитию и предоставлению электронных услуг и сервисов. Таким образом, одной из наиболее важных уязвимостей можно считать информационно-телекоммуникационные системы и сервисы данных компаний. Причём, здесь даже не является принципиальным вопрос о конкретных механизмах реализации несанкционированного доступа к информации со стороны злоумышленников («хакеров»). Сам факт возможности такого доступа, даже если он был совершён лицами с соответствующей подготовкой, уже является сигналом для анализа сетевой инфраструктуры и принятия решений по внедрению программно-технических и программно-аппаратных средств защиты информации.

В целом, как гласят принципы баланса необходимости и достаточности мер защиты, и что также отмечается в исследованиях других авторов [9], выбор и применение состава программно-технических решений определяется совокупностью угроз и характеристиками аппаратной платформы информационной системы. Однако, следует заметить, что для крупных систем затраты на защитные средства, системы и проведение мероприятий контроля защищённости могут оказаться весьма высокими, что приводит к реализации принципа минимализма в реализации защитных механизмов. Можно предположить, что во многих случаях выбор защитных средств и систем основывается больше на идеях формального соответствия требованиям и экономии финансовых средств, не вдаваясь глубоко в состав функций безопасности, предоставляемых теми или иными продуктами.

Тем не менее, логически правильные принципы организации защиты должны быть основаны на понимании того, что одно единственное средство, каким бы хорошим оно не было, является центром атак, и при отсутствии альтернативных (дополняющих или дублирующих) средств защиты не может

давать достаточной уверенности в обеспечении надлежащего уровня защищённости. Аналогично, любой объект, находящийся под защитой одного единственного средства, нельзя расценивать как достаточно защищённый. Обозначим набор возможных средств защиты как x, а набор объектов, подлежащих защите, как y. Тогда реализация и направленность действия защитных средств можно представить моделью двудольного графа (рис. 1). В данном примере показано, что существует, например, 6 объектов защиты и применяется пять защитных средств. Причём, например, функционал средства x_1 позволяет защищать три объекта y_1, y_2 и y_5, а функционал средства x_4 позволяет защищать только один объект y_4. В приведённой модели видно, что все объекты, кроме y_3, защищаются двумя средствами. В этом смысле объект y_3 является наиболее возможным и наиболее вероятным объектом атак. К этому объекту можно также относиться как к наиболее уязвимому. Хотя, справедливости ради, следует заметить, что уязвимость объекта определяется конечно не количеством механизмов, направленных на его защиту, а внутренней структурой этого объекта и его свойствами. И всё же, допускать ситуацию, когда существует объект, защита которого обеспечивается единственным механизмом или средством, не следует. Из того же рисунка видно, что некое средство x_4 применено для защиты лишь одного единственного объекта y_5, что безусловно в реальных ситуациях наводит на мысли о его исключении из системы защиты и экономии соответствующих ресурсов.

Из изложенного анализа предположим гипотезу о том, что наиболее подвержены рискам утечек информации информационно-телекоммуникационные системы крупных компаний, имеющие общие черты, характеризующиеся несоблюдением принципа двойственности или парности построения рубежей безопасности.

Отметим, что двудольные графы оказываются весьма эффективным и наглядным средством построения моделей взаимодействия средств защиты с защищаемыми объектами и находят аналогичное применение и в исследованиях других авторов [10]. Применение данного средства моделирования в совокупности с детальным анализом и формальным описанием функций защиты, позволит найти компромиссное решение о минимизации затрат, не поступаясь принципами обеспечения взаимодействия защитных механизмов. А это в свою очередь требует углублённого анализа и формирования некоего стандартного подхода к формализованному описанию и паспортизации функций защиты, что позволит чётко сопоставлять функциональность систем и выбирать наиболее подходящую их комбинацию индивидуально для каждой системы обработки персональных данных.

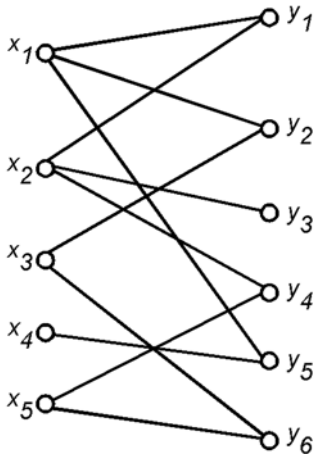

Рис. 1. Модель распределения функций защитных средств на объекты защиты в виде двудольного графа

Рассмотрим, к примеру группу защитных средств, предназначенных для контроля доступа в информационные системы.

Среди таких продуктов можно выделить:

– «Secret Net» (компания «Код безопасности»);
– «Active Roles» (компания «One Identity»);
– «FortiNAC» (компания «Fortinet»);
– «Аккорд» (компания «ОКБ САПР»);
– «Dallas Lock» (компания «Конфидент»).

Даже обзорно сравнивая данные продукты и решения, можно отметить, что они весьма существенно отличаются друг от друга и никак не могут рассматриваться как взаимно альтернативные решения. Тем не менее, для решения задачи контроля доступа необходимо выбрать конкретное решение. Не вдаваясь в оценки популярности, заметим, что продуктовые линейки «Secret Net» и «Dallas Lock» имеют между собой всё же несколько больше общих свойств, и часто рассматриваются как альтернативы. Хотя, ещё раз следует отметить, что во всех перечисленных средствах реализованы свои индивидуальные модели и механизмы противодействия несанкционированному доступу. Кроме того, функциональность продуктов сильно разнится не только между различными производителями (что вполне естественно), но и между различными версиями одного и того же продукта (и здесь может оказаться весьма неприятной неожиданностью, когда в более новой версия продукта может отсутствовать некоторый ранее существовавший функционал), В связи с отсутствием единого формализованного подхода к сравнению функциональных возможностей, целесообразно предложить ряд таких показателей.

Показатель 1 – набор операционных сред функционирования. Существуют продукты, имеющие релизы для различных операционных систем, также как существуют только моносистемные решения.

Показатель 2 – свобода размещения продукта в среде функционирования. Непонятно, почему некоторые разработчики ограничивают возможности выбора пользователем путей к рабочим папкам и папкам инсталляции системы. Для систем, которые не могут быть размещены по нетривиальным путям в системе дискового пространства, этот факт уже можно отметить как их потенциальную уязвимость.

Показатель 3 – набор поддерживаемых типов таблиц разделов, в частности, возможность работы как на MBR, так и на GPT дисках.

Показатель 4 – набор поддерживаемых типов файловых систем (FAT32, NTFS, ReFS, и др.).

Показатель 5 – набор способов и механизмов идентификации и аутентификации пользователей;

Показатель 6 – набор поддерживаемых аппаратных устройств для идентификации пользователей.

Показатель 7 – наличие средств доверенной загрузки и создания доверенной среды.

Показатель 8 – набор алгоритмов прозрачного шифрования хранимой информации.

Показатель 9 – набор уровней прозрачного шифрования хранимой информации (шифрование физического диска как объекта, шифрование логического диска как объекта, шифрование папки как объекта, шифрование файла как объекта, и т.п.).

Показатель 10 – состав функции контроля целостности программной конфигурации (системных файлов, файлов пользователя, реестра, загрузочных секторов, и т.п.).

Показатель 11 – набор механизмов контроля целостности файлов (длина, дата, время, контрольная сумма, место физического размещения на диске, и т.д.).

Показатель 12 – состав функции контроля целостности аппаратной конфигурации (номер процессора, системной платы, код жёсткого диска, и т.д.).

Показатель 13 – набор поддерживаемых моделей управления доступом (ролевая, мандатная, дискреционная).

Показатель 14 – набор функций запрета действий (запрет видимости файлов, запрет запуска, запрет изменений, запрет чтения, и т.п.)

Показатель 15 – набор параметров логирования событий (перечень фиксируемых атрибутов).

В данной работе не ставится цель разработать функционально завершённую систему унифицированных сопоставимых для сравнительного анализа показателей, это планируется в качестве отдельного исследования. Поэтому предложенный на данном этапе перечень из 15 показателей можно рассматривать как начальный, но следует отметить, что он составлен из принципа дискретности: каждый показатель имеет набор конкретных возможных дискретных значений, что даст возможность проводить быстрое аналитическое сопоставление функциональности системы, накладывая их на задачи обеспечения безопасности для каждого конкретного случая.

Обеспечение безопасности сетевой инфраструктуры обработки персональных данных не может быть обеспечено лишь средствами защиты от несанкционированного доступа. В составе данных средств нет специфичных функций безопасности сетевой инфраструктуры и противодействию внешним нарушителям, в том числе осуществляющим попытки реализации сетевых атак.

В зависимости от конфигурации системы обработки персональных данных, в компоненты единого комплекса средств защиты могут входить следующие виды продуктов (но не ограничиваясь ими):

– средства контроля и управления доступом (в частности, рассмотренные выше «Secret Net» и «Dallas Lock»);

– средства доверенной загрузки;
– средства анализа сетевого трафика;
– средства защиты веб-ресурсов;
– системы обнаружения и предотвращения вторжений;
– системы построения защищённых виртуальных корпоративных сетей;
– межсетевые экраны;
– антивирусные продукты;
– системы предотвращения утечек информации, контроля и мониторинга действий пользователя и контроля съёмных машинных носителей;
– средства анализа защищённости.

В организациях, использующих распределённые информационные системы [11, 12], в том числе собственной разработки [13], и в том числе с предоставлением доступа клиентам по веб-интерфейсам и/или предоставляющим доступ сотрудникам с удалённых рабочих мест, необходимо создание защищённых каналов передачи обрабатываемой информации. Для этих целей целесообразно применение средств и систем, формирующих защищённую виртуальную корпоративную сетевую инфраструктуру. Среди таких продуктов подобного назначения можно выделить:

– комплекс программных компонентов «VipNet» (компания «Инфотекс»), состоящий из «VipNet Coordinator», «VipNet Administrator», «VipNet Client»;
– программно-аппаратный комплекс «Застава» (компания «Элвис-Плюс»);
– программно-аппаратный комплекс «С-Терра TLS» (компания «С-Терра СиЭсПи»);
– программно-аппаратный комплекс «Атликс-VPN» (компания «НТЦ Атлас»);
– программно-аппаратный комплекс «Континент» (компания «Код безопасности»);
– программно-аппаратный комплекс «КриптоПро NGate» (компания «Крипто-ПРО»).

Указанные продукты в целом предназначены для создания защищённых корпоративных сетей с шлюзами безопасности, обеспечивающими туннелированные каналы связи для взаимодействия с удалёнными узлами и пользователями.

Выбор решения для построения VPN ещё более сложен, по сравнению, например, с выбором средств защиты от несанкционированного доступа. Это объясняется целым рядом причин:

– наличием, как правило, аппаратной части в комплексе построения VPN с шлюзами безопасности;
– в свободном доступе не всегда есть полная документация на продукты;
– не все решения пригодны для развёртывания на Linux-подобных операционных системах.

В отношении последнего пункта можно отметить, что для платформ на базе ОС Linux и её производных популярным выбором часто являются продукты с открытым исходным кодом, в частности «OpenVPN», «PPTP», «IPSec». При их применении есть определённые недостатки:

– возможны несовместимости между версиями продуктов и операционных систем, в том числе неявные несовместимости скрытого характера;
– отсутствует сертификация по требованиям безопасности, установленным в регламентирующих документах.

Ещё одной сложностью является различие в понятийном аппарате различных разработчиков программного обеспечения, когда одноимённые функции безопасности имеют различные принципы действия. Например, в подавляющем большинстве решений по построению VPN под туннелем подразумевают P-to-P-соединение между криптошлюзами, в тоже время в линейке продуктов «ViPNet» под туннелями понимается соединение между хостами (рис. 2) [14].

Рис. 2. Пример различия в терминологии функций безопасности у различных разработчиков

Квалифицированный выбор программных и (или) программно-аппаратных средств осложняется уже рассмотренной ранее проблемой отсутствия формализованных унифицированных дискретных показателей и характеристик функций безопасности продуктов, что в сочетании с неполной или даже

полной, но очень объёмной документацией не позволяет найти наиболее оптимальное решение по выбору защитных средств.

В связи с отсутствием унифицированного перечня функций безопасности и показателей аналитического сопоставления систем, при создании систем защиты персональных данных специалистами, не имеющими дополнительной углублённой профессиональной подготовки по вычислительным сетям и сетевой безопасности, возникают вопросы, не находящие наиболее оптимального разрешения в установленные сроки. Например: нужен ли дополнительный (возможно, программно-аппаратный межсетевой экран), если разворачивается защищённая корпоративная сеть на базе комплекса продуктов ViPNet? Или, есть ли необходимость внедрения в корпоративную инфраструктуру отдельных средств предотвращения утечек конфиденциальной информации (DLP-систем) [15], если уже имеется развёрнутый комплекс «Secret Net» либо «Dallas Lock», которые хоть и не перекрывают весь функционал систем DLP типа «СёрчИнформ КИБ», но имеют функции администрирования доступа к портам ввода-вывода и приводам оптических дисков?

Ещё ситуация: предположим, в компании уже закуплено и внедрено необходимое количество лицензий антивирусного продукта второго класса (например, от компании «Лаборатория Касперского»), а затем было принято решение внедрить комплексную систему защиты информации «Secret Net Studio», которая также имеет в себе интегрированный антивирусный модуль, правда четвёртого класса. Для защиты персональных данных любого уровня защищённости, пригодны антивирусные продукты и второго, и четвёртого класса. И следует разрешить ситуацию, которая имеет как минимум три возможных пути:

А) отказаться от первого продукта в пользу комплексной системы, согласившись с допустимым понижением класса антивирусной защиты;

Б) не использовать антивирусные функции комплексного продукта, обеспечивая антивирусную защиты средствами отдельного специализированного средства;

В) совместить оба продукта, настроив одновременную совместную работу обоих антивирусных модулей.

Два последних пути выглядят наиболее заманчивыми, но могут привести к проблемам, связанным с программными конфликтами и заметным повышением нагрузки на вычислительную систему. А может быть, какое-то из двух имеющихся антивирусных решений обладает такими возможностями, которые окажутся крайне полезными для защищаемой информационной системы?

И, наконец, обратимся к вопросу анализа защищённости информационных систем персональных данных. Статья 18.1 Федерального Закона «О персональных данных» в качестве перечня мер по обеспечению защиты персональных данных определяет проведение оператором персональных данных внутреннего контроля и (или) аудита. Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01.11.2012 конкретизирует, что оператором самостоятельно либо с привлечением внешних специалистов должен проводиться контроль выполнения требований по защите персональных данных. Не обсуждая вопросы организационного контроля, в контексте оценки безопасности функционирования сетевой инфраструктуры возникает задача проведения инструментального аудита безопасности информационно-телекоммуникационной сети оператора. Методические аспекты проведения аудита является предметом отдельных исследований [16], однако также необходимо чётко и однозначно определить совокупность показателей безопасности, которые могут быть исследованы.

Совершенно очевидно, что для методичного рассмотрения поставленных проблемных ситуаций необходимо критериальное сопоставление функционала программных средств, что требует единообразного подхода к описанию функций безопасности. Отсутствие такой формализованной системы показателей безопасности существенно осложняет проведение квалифицированного анализа возможных решений по построению системы защиты персональных данных и определению наиболее оптимального сочетания программно-аппаратных средств.

В свою очередь, создание унифицированной системы формализованного описания функций безопасности позволит применить методы метамоделирования [17] для интеграции систем безопасности как между собой, так и во взаимодействии с защищаемой информационной системой.

Заключение

На основе проведённого исследования выдвинута гипотеза об общих свойствах информационных систем персональных данных крупных компаний, наиболее подверженных рискам утечек конфиденциальной информации.

Можно сделать предположительный вывод о недостаточно полном перекрытии угроз безопасности средствами и механизмами программно-технической и аппаратно-программной защиты. Повышение уровня защищённости сетевой информационной инфраструктуры следует осуществлять в том числе за счёт организации взаимодействия защитных механизмов с взаимным дополнением и дублированием функций, которые можно рассматривать как парные или уровневые рубежи защиты.

Проведённый анализ совокупности аппаратно-программных продуктов, применяющихся для построения систем защиты персональных данных показал, что на основе обобщённой информации практически невозможно провести квалифицированный выбор наиболее подходящего комплекса защитных средств. Защита персональных данных в крупной сетевой инфраструктуре требует применения широкого номенклатурного спектра средств обеспечения безопасности, включая средства защиты от несанкционированного доступа, системы построения виртуальных корпоративных сетей, антивирусные продукты, межсетевые экраны, системы обнаружения вторжений, и др.

Можно отметить, что функциональные возможности защитных продуктов в деталях настолько разнообразны, что представляет серьёзное затруднение их сопоставительный анализ и совместная интеграция в единую систему защиты персональных данных.

Решение проблемы интеграции защитных средств между собой и во взаимодействии с информационными системами может быть осуществлено с применением подхода метамоделирования, для чего не необходимо определить унифицированную систему формализованного представления функций безопасности и их дискретные наборы показателей.

Литература

1. *Сиротский А.А*. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде // Технологии техносферной безопасности. 2013. № 4(50). С. 18. EDN SCCPQV

2. *Сиротский А.А.* Информационные и методические проблемы информационной безопасности личности в современном деловом обороте. «Системы безопасности – 2015». Материалы 24-й международной научно-технической конференции (26 ноября 2015 г., Москва). М.: Академия ГПС МЧС России. 2015.

3. *Балаев Р.С*. Факторы рисков и угроз экзистенциальной безопасности личности в информационном обществе. Наука XXI века: новый подход. Материалы XIV молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. Научно-издательский центр «Открытие». 2015. С. 56-63.

4. *Сиротский А.А*. Анализ изменений законодательства о персональных данных, вступающих в силу с 1 сентября 2022 г. // Безопасность информационных технологий, [S.l.], т. 29, № 4. С. 67-81, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1450. DOI: http://dx.doi.org/10.26583/bit.2022.4.06.

5. *Сиротский А.А., Самадуров А.Э.* Тенденции развития информационных сервисов в структуре цифровой экономики // Современные информационные технологии в образовании, науке и промышленности: XI Международная конференция, IX Международный конкурс научных и научно-методических работ, Москва, 02-03 ноября 2018 года / Ответственные редакторы: Т.В. Пирязева, В.В. Серов. М.: ООО "Издательство "Спутник+", 2018. С. 169-172. EDN YWFBJB

6. *Сиротский А.А*. Информационная безопасность систем дистанционного банковского обслуживания // Современные инструментальные системы, информационные технологии и инновации: сборник научных трудов XI Международной научно-практической конференции: в 4-х томах, Курск, 19-21 марта 2014 года. Курск: Закрытое акционерное общество "Университетская книга", 2014. С. 101-105. EDN RCBHZP

7. *Sirotskiy A.A*. Information Security of the Automated Systems of Financial Credit Institutions // Contemporary Problems of Social Work. 2016. Vol. 2. № 2(6), pp. 185-193. DOI 10.17922/2412-5466-2016-2-2-185-193. EDN WXPDWT

8. «Сравни.ру». 14 компаний, откуда утекли данные пользователей в 2022 году. URL: https://www.sravni.ru/text/14-kompanij-otkuda-utekli-dannye-polzovatelej-v-2022-godu. (Дата обращения 27.01.2023).

9. *Осовецкий Л.Г., Птицын А.В*. Проблемы построения комплексных систем защиты информации от несанкционированного доступа в телекоммуникационных системах // Известия ТРТУ. 2003. № 4(33). С. 116-118. EDN KVHQYV

10. *Шляпкин А.В.* Математическое моделирование процессов защиты информации для мобильных устройств // Наука – промышленности и сервису. 2014. № 9-1. С. 160-164. EDN VDREZT

11. *Сиротский А.А*. Распределенные системы. Организация и типология // Техника машиностроения. 2012. № 2(82). С. 34-37. EDN RURSLL

12. *Sirotsky A.A., Zvereva A.O*. The distributed systems: modern representations and development tendencies // Объектные системы. 2011. № 4, pp. 21-26. EDN THDXNJ

13. *Сиротский А.А.* 77-48211/616336 Инструменты разработки облачных распределённых ERP-систем управления ресурсами предприятия // Инженерный вестник. 2013. № 9. С. 15. EDN ROFCMJ

14. ViPNet в деталях: разбираемся с особенностями криптошлюза. // Блог компании Ростелеком-Солар. URL: https://habr.com/ru/company/solarsecurity/blog/514896/.(Дата обращения 27.01.2023).

15. *Сиротский А.А., Деревянко С.С.* Краткий взгляд на применение DLP-систем в медицинской организации // Современные проблемы информационной безопасности и программной инженерии : Сборник избранных статей научного семинара №1(6) кафедры информационной безопасности и программной инженерии, Москва, 24 января 2014 года / Российский государственный социальный университет, кафедра информационной безопасности и программной инженерии. М.: Общество с ограниченной ответственностью "Сам Полиграфист", 2014. С. 34-38. EDN UYKYFL

16. *Сиротский А.А., Резниченко С.А.* Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий. 2021. Т. 28. № 3. С. 103-117. DOI 10.26583/bit.2021.3.09. EDN LSDPLE

17. *Ворошилова О.С., Сиротский А.А.* Интеграция информационных систем на основе метамоделирования // Информационная безопасность бизнеса и общества: Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности / Российский государственный социальный университет. М.: Издательство "Перо", 2016. С. 18-22. EDN VNKRIF

ПРЕДУПРЕЖДЕНИЕ АТАК, БАЗИРУЮЩИХСЯ НА SQL-ИНЪЕКЦИЯХ

Яковенко Наталья Викторовна,
Московский Технический Университет Связи и Информатики,
старший преподаватель кафедры СИТиС, Москва, Россия
nv1906.iakovenko@yandex.ru

Чижова Екатерина Михайловна,
Московский Технический Университет Связи и Информатики, бакалавр гр. БСТ1903, Москва, Россия
bst1903@ya.ru

Тремасова Лилия Андреевна,
Московский Технический Университет Связи и Информатики,
магистрант М092101(75), Москва, Россия
lila.trem@yandex.ru

Гадасин Даниил Денисович,
Московский Технический Университет Связи и Информатики, бакалавр гр. БСТ2103, Москва, Россия
gadasin115@gmail.com

Аннотация

Информационная безопасность сейчас является одним из основных приоритетов человечества, жизнь любого в нашем обществе связана с информационными технологиями. При атаке на какой-либо программный продукт могут быть украдены личные данные, денежные средства или нанесен другой урон. Безопасность программного обеспечения зависит от многих факторов, но основными являются сам язык программирования и разработчик. В данной работе рассмотрены основные уязвимости языков программирования, как, используя их, кибер-злоумышленник наносит вред, а также какие функции уже предусмотрены в языках программирования для смягчения угроз и какие меры может предпринять программист.

Ключевые слова: *безопасность, языки программирования, уязвимости ЯП, атаки, SQL-инъекции, функции безопасности*

Введение

Спрос на приложения растет в геометрической прогрессии, что заставляет программистов делать огромную работу в кратчайшие сроки, вследствие чего они обычно даже не задумываются о том, какие уязвимости есть в используемом языке программирования, что необходимо делать для предотвращения кибератак злоумышленников. Атаки могут быть самыми различными, их можно разделить на: межсайтовый скриптинг, атаки с проверкой ввода, переполнение буфера [1] и атаки возвратно-ориентированного программирования [2].

Об этих атаках исследователям известно, они в свою очередь стремятся обезопаситься различными методами, например, целостностью потока управления в компиляторе рандомизация расположения адресного пространства и стековые канарейки на уровне операционной системы и многие другие методы на различных уровнях. Но все эти методы не обеспечивают абсолютной защиты, злоумышленники все равно находят лазейки для совершения атак. Это происходит потому, что методы смягчения не заменяют уязвимый код, вместо этого эти методы пытаются уменьшить общий эффект эксплуатации памяти.

В данной статье определены уязвимости и текущее состояние функций безопасности в самых популярных на сегодняшний день языках программирования. А также, на основе данных исследований получен вывод о безопасности современных систем.

Уязвимости в языках программирования

Какие цели преследует кибер-злоумышленник? У каждого злоумышленника цель может быть своя, но большинство из них сводятся либо к получению несанкционированного доступа, либо к внесению изменений в веб-интерфейс с помощью отказа в обслуживании [14-19]. Главными источниками

уязвимостей на сегодняшний день являются языки программирования, но, к сожалению, программисты зачастую о них не знают и даже не задумываются о защите своего программного продукта от атак связанных с незащищенностью языков программирования.

Одна из основных проблем большинства уязвимостей заключается в испорченном вводе, поэтому ему никогда нельзя доверять, он должен быть надлежащим образом проверен по типам и диапазону. В противном случае возможны такие атаки, как переполнение буфера, возвратно-ориентированное программирование и атаки SQLI. Но уязвимости бывают и в других места, атаки нацелены на разные уязвимости.

Атака с внедрением SQLI происходит через веб-форму, которая не может должным образом проверить входные данные. К тому же, БД часто возвращает сообщения, содержащие информацию об ошибке, при некорректном запросе или других проблемах, однако, если такое сообщение попадет в руки злоумышленника, то это может стать для него полезным.

Для того, чтобы избежать атак, связанных с внедрением постороннего кода в пользовательский запрос, чаще всего применяются шаблоны SQL-запроса. При использовании данного метода клиент вводит только изменяемую переменную и больше ни к чему доступа не имеет, запрос выстраивается безопасным образом. Но для использования данной защиты необходимо приложить не мало усилий программисту: ему предстоит реорганизовать запрос и определить его основу. Существуют и другие методы по смягчению атак, например, проверки запроса использовать SQLCheck, все символы запроса разделить на кодовые и не кодовые. Однако, атаки этого вида до сих пор существуют, мошенники находят пути обхода известных методов, а также сами методы имеют ограничение в использовании.

С помощью различных методов кибер-злоумышленник может добиться переполнения буфера [3]. Для чего ему это необходимо? Когда буфер обмена заполнен происходит изменение адреса возврата, при этом есть возможность сделать так, чтобы теперь указатель был на адрес полезной нагрузки злоумышленника. После таких махинаций злоумышленник может добиться сбоя служб или повышения привилегий [4], а также повредить программу.

Веб-приложения ограничивают доступ сценариев, работающих от имени других доменов, к файлам cookie, зарегистрированным для этих доменов. Однако этот простой механизм предотвращения можно обойти с помощью XSS. Злоумышленник может разместить созданный сценарий на доверенном вебсайте, который впоследствии будет выполнен другим пользователем того же сервера. Вредоносный код выполняется на клиентском компьютере жертвы, что позволяет злоумышленнику прочитать значение файла cookie аутентификации. Значение файла cookie аутентификации состоит из учетных данных пользователя для сеанса, таких как идентификатор сеанса. Злоумышленник может легко перехватить сеанс пользователя, используя информацию, хранящуюся в файлах cookie аутентификации.

XSS также занимает первое место в списке атак OWASP. Веб-серверы могут использовать безопасные флаги и флаги HttpOnly, чтобы избежать доступа к файлам cookie со стороны клиентского сценария.

Время проверки по времени использования (TOCTOU) — это ошибка, вызванная состоянием гонки, которая возникает, когда синхронизация не была запрограммирована должным образом. Подходы обычно предназначены для последовательных программ, а не для параллельных программ. Такие методы, как отслеживание испорченных данных или обеспечение безопасности памяти, отслеживают данные программы с помощью тегов испорченных данных или границ массива соответственно. Если в отслеживаемой программе есть состояние гонки, то защитная техника становится небезопасной. Переменные необходимо проверять и использовать атомарно, если имеется такая возможность, так как это путь к избеганию TOCTOU. Языки программирования, которые поддерживают многопоточность, нуждаются в тщательной синхронизации, программист должен предусмотреть все нюансы для избегания состояния гонки. Одним из таких языков является Java.

У каждого пользователя есть личная и конфиденциальная информация, она может содержаться как на смартфоне, так и внутри какого-либо веб-приложений, как на компьютере, так и на сменном носителе [5], вариантов множество. Когда пользователь выгружает личную информацию куда-либо, то он рассчитывает на сокрытие его данный, согласно политике конфиденциальности, но при нарушении данной секретности происходит и нарушение прав пользователя. Раскрытие конфиденциальных данных входит в топ-10 списка OWASP. Для защиты конфиденциальных данных существует TaintErase. Принцип работы данного метода заключается в динамическом отслеживании испорченных данных, что происходит на уровне приложения, как только они обнаруживаются, происходит замена

случайными байтами, а на уровне ядра в пользовательском пространстве имеется список испорченных файлов. Но данный метода является не совсем удобным для постоянного использования, так как пользователь должен самостоятельно заранее выделить те файлы, которые являются конфиденциальными.

Аутентификация зачастую является уязвимым местом приложения, а ее нарушение может позволить кибер-злоумышленнику стать законным пользователем. Пароли и имена часто длинные и сложные, не редко они создаются автоматическими средствами генерации, а пользователи – это обычные люди, которые и так постоянно находятся в потоке информации и уже не могут запомнить множество имен и паролей, поэтому прибегают к использованию единого входа (SSO). Для защиты аутентификации чаще всего прибегают к сохранению сеансов, долгосрочному управлению учетными данными пользователей. Также при создании собственного приложения лучше прибегнуть к использованию существующего механизма аутентификации, поскольку он проверен временем и множеством специалистов, а при самостоятельном программировании можно упустить важные моменты.

Для борьбы с кибератаками было предложено множество решений по смягчению последствий. Эти решения могут быть основаны на компиляторе, встроены в операционные системы, аппаратные решения, методы отслеживания испорченных данных или методы перезаписи/инструментирования двоичных файлов. Все предложенные выше методы не могут полностью устранить угрозу вторжения в ПО. Это происходит из-за того, что большинство программистов не используют методы безопасного кодирования из-за спешки или некомпетентности в данном вопросе. Конечно, можно было бы сейчас посвятить разработчиков во все нюансы и переписать код, но старых кодов невероятное количество, поэтому миссия невыполнима и нерациональна. Чтобы не переписывать старый код необходимо менять сами языки программирования, путем доработок устранять уязвимости, а программистов оповещать о возможных пробелах в безопасности, а также уделять больше времени самым уязвимым местам. В следующем разделе сказано, каким образом можно уберечь программный продукт от самых популярных и опасных атак, какие функции для этого уже включены в языки программирования, а о каких стоит позаботиться разработчику.

Разработчики языков программирования стремятся уменьшить количество уязвимостей, а также снять с разработчиков ПО часть ответственности за безопасность. С этой целью разработаны различные функции на уровне приложения [6], основные из которых рассмотрены ниже.

Исключения или ошибки считаются аномальными событиями [7], указывающими на то, что внутреннее состояние системы повреждено и требуется либо восстановление программного обеспечения, прежде чем система продолжит свою нормальную работу, либо выводится соответствующее сообщение для пользователя с указание действий. Веб-приложение должно обрабатывать ошибки собственного приложения и не должно полагаться на сервер. Надлежащая обработка ошибок в языках программирования предотвращает утечку ресурсов, которая может поставить под угрозу безопасность приложения.

Обработка ошибок часто объединяется с механизмом ведения журнала (это средство отладки и диагностики), который содержит конфиденциальную информацию [8]. Языки Java, Python и C# хранят журналы в открытом виде. Это уязвимость, поскольку хранение журналов в виде простого текста дает доступ злоумышленникам к информации, которая может быть использована для кибер-атак. В журнале не должно быть исполняемого кода.

Журналы могут быть детализированы с различной точностью [9]. Это делается для соблюдения баланса между экономией ресурсов и облегчением отладки. Функция уровня журнала позволяет разработчикам выбирать уровень детализации информации для регистрации. Чаще всего для разных блоков выбираются различные уровни детализации. Во всех популярных языках программирования есть библиотеки для данных целей.

Сообщения об ошибках не должны содержать ценной информации, таких как сведения о неправильном имени пользователя и пароле. Разработчикам всегда доступно свойство Stacktrace, которое показывает последовательность вызовов функций, приводящих к подробному сообщению об ошибке.

Надлежащая проверка входных данных может предотвратить различные атаки, связанные с входными данными, вызванные непроверенными запросами к базе данных, ненадежными пользовательскими входными данными, переполнением размера входного буфера и отсутствием проверки выходных данных [10,11,12]. Эта функция безопасности имеет подфункции, такие как безопасность запросов к базе данных, безопасность ввода данных пользователем, размер входного буфера и закодированный вывод.

Алгоритм совершения атаки и атаки на основе SQL инъекций

Почти все программные приложения полагаются на базу данных для управления данными, которые обрабатываются в этом приложении, на этом уровне организуется бизнес-логика. База данных хранит организационные данные, политики, параметры конфигурации и разрешения. Бизнес-логика обычно реализуется на уровне базы данных. Ошибки программирования в компонентах кода базы данных могут привести к серьезным уязвимостям, которые могут привести к SQLI или другим атакам проверки ввода. Библиотеки аннотаций данных обычно состоят из регулярных выражений для проверки данных.

Процедура SQLI начинается с веб-интерфейса, который используется для отправки входных данных пользователя на внутренний сервер. Выявив неадекватные проверки в полях ввода, злоумышленник распознает возможность SQLI. SQLI часто используется для получения доступа к системе, обходя механизмы безопасности. Этого можно добиться, вставив вредоносный запрос во входные данные пользователя, которые при обработке всегда возвращают истинное условие. Схема атаки:

1. Внедрение вредоносных SQL-запросов через поля ввода пользователя.
2. Изменение существующих SQL-запросов, добавление вредоносного запроса, получение из веб-интерфейса (злоумышленника) через HTTP-запрос.
3. Выполнение новой вредоносной инструкции SQL на сервере базы данных.

Данную схему можно увидеть на рисунке 1.

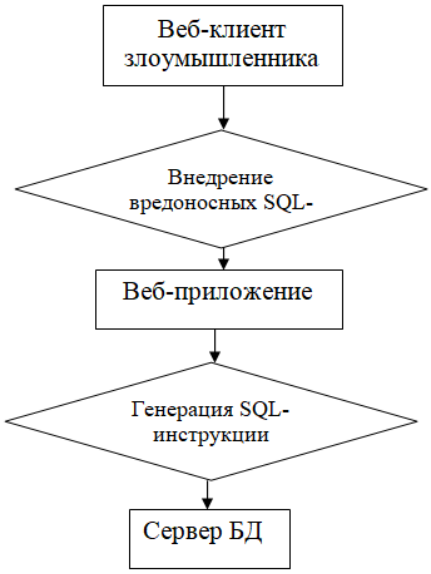

Рис. 1. Схема атаки

Атаки с использованием SQL-инъекций можно в целом разделить на следующие три категории:

1. SQL-инъекция на основе объединения
2. SQL-инъекция на основе ошибок
3. Слепая SQL-инъекция
4. SQL-инъекция на основе логических значений
5. Атаки SQL-инъекций, основанные на времени (рис. 2)

Современный метод предотвращения атак SQL Injection – хеширование запросов. В методе хеширования запроса хэш-значение сгенерированного запроса будет сравниваться с хэш-значением легитимного запроса. Этот метод прост в использовании с любым языком или типом базы данных. Хэш используется для проверки сохранения целостности данных.

При таком подходе будет создан массив, состоящий из хэшей законных запросов (пример: SELECT, INSERT, DELETE, ALTER). Эти запросы будут включать только абстрактную форму функции базы данных. После этого будет сгенерирован хэш этих запросов, и его значение будет сохранено в коде. При получении запроса значения атрибутов изменяются с помощью регулярных выражений и алгоритмов замены на пустое или любое другое заданное значение.

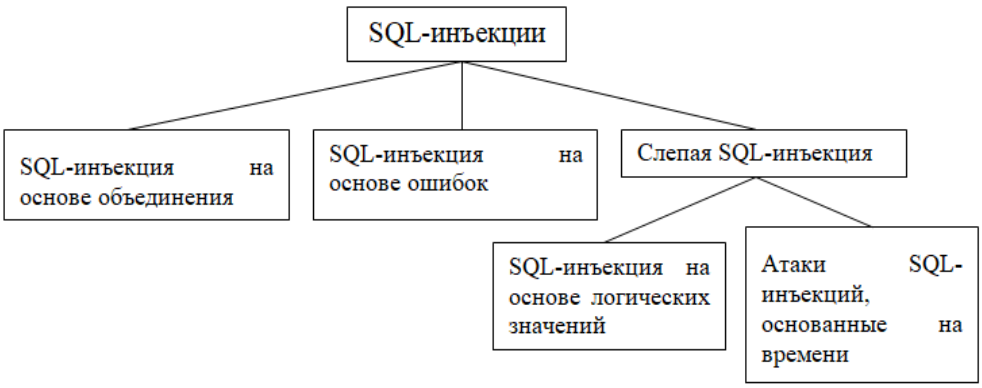

Рис. 2. Виды SQL-инъекций

После этого этот запрос будет хеширован, и будет проведено сравнение между ним и ранее вычисленным хэшем действительного запроса. Если этот хэш будет успешно сопоставлен, запрос продолжится; в противном случае оно было бы отклонено. Любой запрос SQLI, содержащий вредоносную полезную нагрузку, приведет к тому, что сервер отклонит запрос, поскольку его хэш не будет соответствовать заранее определенной полезной нагрузке.

Этот метод разрабатывает решение для веб-уязвимости, известной как SQL-инъекция, с использованием алгоритма сопоставления строк и хеширования. Даже если база данных скомпрометирована, злоумышленнику вряд ли удастся обнаружить настоящие данные, поскольку хэш-значения хранятся в базе данных. Хеширование используется в этой реализации в качестве функции безопасности для снижения вероятности атак. Работа метода представлена на рисунке 3.

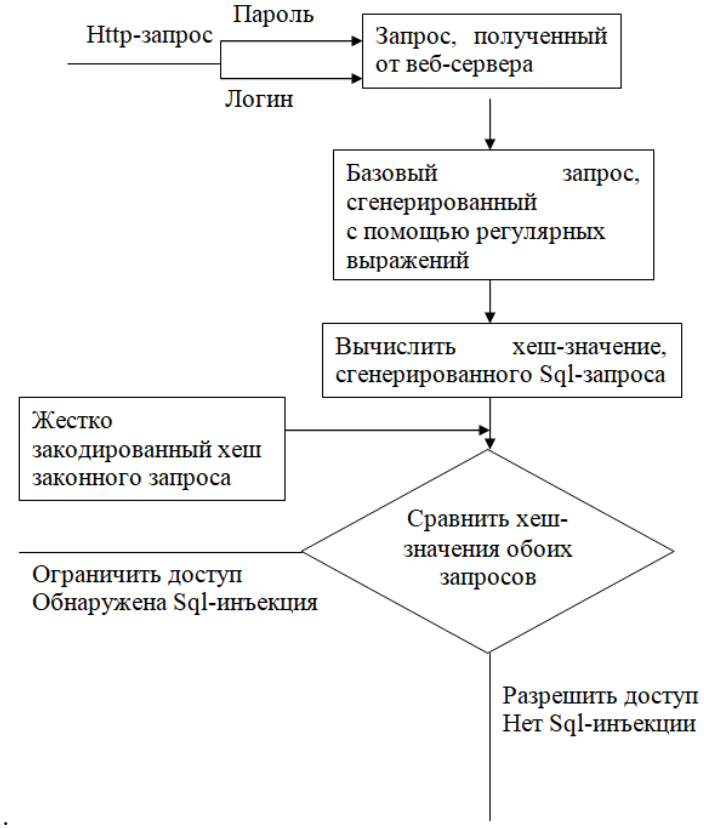

Рис. 3. Метод хеширования запросов

Модель прогнозирования, основанная на машинном обучении, была предложена М. О. Адебийи в качестве инструмента предотвращения и обнаружения SQL-атак и уязвимостей с использованием алгоритмов хи-квадрата с тремя категориями: KNN, Дерево решений и Наивный Байесовский алгоритм, а также метод оценки производительности разработанной модели [13].

В рамках этого исследования рассматриваются три важные процедуры; набор данных, полученный университетом Нью-Брансуика, выбор признаков хи-квадрата, процесса и дерева решений. На приведенной ниже на рисунке 4 диаграмме показана общая процедура упомянутого исследования.

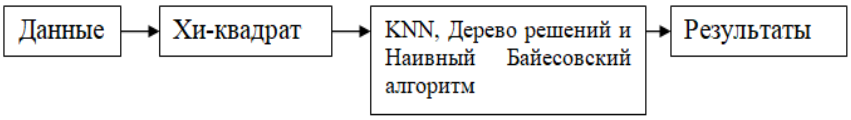

Рис. 4. Диаграмма модели прогнозирования, основанная на машинном обучении

Путем анализа всевозможным методов был выбран тот, который и предлагается для использования в данной работе: метод обнаружения SQL-инъекций с использованием глубокого леса, который включает в себя два важных этапа: первый – этап автономного обучения, а второй – этап онлайн-тестирования. Данные для обучения извлекаются из уязвимой платформы с использованием приманки механизма безопасности и образцов SQL-инъекций в качестве первого этапа автономного обучения. Затем модуль подготовки данных предварительно обрабатывает закодированные образцы, чтобы обеспечить декодирование, прежде чем подавать их в модуль извлечения признаков. После процедуры извлечения признаков, которая рассматривает атрибуты: ключевые слова SQL-инъекций, длина оператора инъекции, числовые символы, символы верхнего регистра, нулевые символы, специальные символы и аннотации — модель глубокого леса получает входные данные из этих векторов признаков. Чтобы построить тот же вектор измерений, что и на этапе автономного обучения, когда дело доходит до этапа онлайн-тестирования, необнаруженные операторы SQL должны быть сначала расшифрованы компонентом предварительной обработки данных, а затем введены в компонент извлечения признаков. Наконец, обученная модель будет использоваться для определения того, является ли SQL-запрос вредоносным или нет. Схема работы данной модели показана на рисунке 5.

Рис. 5. Метод обнаружения SQL-инъекций с использованием глубокого леса

После блока «Старт» происходит сбор данных, они предварительно сохраняются в БД и фиксируются в отчетах, далее проходят предварительную обработку – очистку, из обработанных данных происходит сбор признаков и классификация, далее происходит аутентификация пользователей, что способствует

предотвращению атак. Финальным этапом является проверка доступа пользователя, если все данные введены корректно, то предоставляется доступ, в противном случае запрос отклоняется.

Заключение

Разработчику необходимо знать об известных уязвимостях в языке прикладного программирования, поскольку он создает программное обеспечение с использованием этого языка. Реализацией разработки занимается программист, в своем большинстве, программисты не владеют навыками защищенного написания текстов программ. Несмотря на то, что реализация скрипта, в котором отсутствуют уязвимости, непосредственно относятся к вопросам программирования, не все зависит от квалификации программиста. Одной из проблем являются как известные, так и скрытые уязвимости в самих языках программирования. Данные уязвимости могут быть задействованы с помощью кибератак или путем подмены в SQLзапросе. Таким образом, если разработчик какого-либо языка программирования знает о возможных уязвимостях, то ему необходимо предусмотреть действия, которые позволят свести до нуля возможности кибер-преступников.

Помимо этого, он тем самым облегчает труд программиста, у которого пропадает необходимость отслеживать корректность кода в рамках самого языка. Анализ скрытых «окон» для совершения противоправных действий, имеющихся в таких языках программирования как C++, C#, Java, Pythoni Rubyпоказал, что они имеют достаточно высокий уровень безопасности, который в них был заложен разработчиками, но в языке C++ уровень безопасности все же несколько ниже по отношению к другим языкам при использовании атак, базирующихся на внедрении в запрос вредоносного SQLкода.

Литература

1. *Тернер С*. Уязвимости безопасности десяти самых популярных языков программирования: C, Java, C++, Objective-C, C#, PHP, Visual Basic, Python, Perl иРубин. Дж Технол Рез. 2014. 5, pp. 1-17.

2. *Марпаунг Дж.А., Сайн М., Ли Х.Дж.* Обзор методов обхода вредоносного ПО: современное состояние и проблемы. Материалы 14-ойМеждународная конференция по передовым коммуникационным технологиям (ICACT); 19-22 февраля 2012 г.; Пхенчхан, Южная Корея, pp. 744-749.

3. *Гадасин Д.В., Шведов А.В., Усачева Д.И.* Механизмы обеспечения безопасности маршрутизации в сети Интернет // III Научный форум телекоммуникации: теория и технологии TTT-2019 : Материалы XXI Международной научно-технической конференции, Казань, 18-22 ноября 2019 года. Том 1. Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. С. 292-293. EDN OSAFRG

4. *Гадасин Д.В., Веденеев П.С., Шведов А.В*. Уязвимости системы маршрутизации глобальной сети Интернет и возможные пути их преодоления // Перспективные технологии в средствах передачи информации – ПТСПИ-2019 : Материалы XIII международной научно-технической конференции. В 2-х томах, Владимир, 03-05 июля 2019 года / Редколлегия: А.Г. Самойлов [и др.]. Том 1. Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2019. С. 94-96. EDN YFEIAH

5. *Гадасин Д.В., Пантелеева К.А.* Работа с данными в условиях антироссийских санкций // Цифровая трансформация промышленности: новые горизонты : Сборник научных трудов по материалам 3-й Всероссийской научно-практической конференции, Москва, 10 ноября 2022 года. Том 1. М.: ООО "Русайнс", 2022. С. 115-119. EDN UYEPWI

6. *Шведов А.В., Гадасин Д.В., Коровушкина В.М., Мелькова Е.К*. Интеллектуальное тестирование как способ повышения качества информационной системы // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12. № 2. С. 43-52. EDN GOLZGE

7. *Алешинцев А.В., Сак А.Н.* Моделирование информационных систем с помощью методов теории графов // Технологии информационного общества : Сборник трудов XII Международной отраслевой научно-технической конференции, Москва, 14-15 марта 2018 года. Том 2. М.: Издательский дом Медиа Паблишер, 2018. С. 40-43. EDN XTOTOX

8. *Иванов О.В., Шведов А.В., Веденеев П.С*. Влияние уязвимости системы маршрутизации на интернет вещей // Телекоммуникационные и вычислительные системы - 2019 : Труды международной научно-технической конференции, Москва, 20 ноября 2019 года. М.: Горячая линия − Телеком, 2019. С. 276-279. EDN QQHSWO

9. *Zolotukhin P.A., Melkova E.K., Gadasin D.V., Korovushkina V.M*. Using Intelligent Testing as a Tool to Improve the Quality of Transport Information Systems // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings, Moscow, 15-17 марта 2022 года. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744348. EDN NOMJLX

10. *Алыев Ш.З., Гадасин Д.Д., Шведов А.В*. Анализ показателей устойчивости в корпоративных сетях и возможные пути её повышения // Перспективные технологии в средствах передачи информации : материалы 14-ой международной научно-технической конференции, Владимир, 06–07 октября 2021 года. Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2021.

С. 415-418. EDN QPGQOA

11. *Maklachkova V.V., Shvedov A.V., Alyev S.* Analysis of Resilience Indicators in Corporate Networks and Possible Ways to Improve It // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings, Moscow, 15-17 марта 2022 года. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744353. EDN ZRMVJS

12. *Шведов А.В., Савин В.А., Мартынов М.Д.* Разработка приложения для синтаксического анализа сформированных в базу структурированных данных // Технологии информационного общества : Сборник трудов XVI Международной отраслевой научно-технической конференции, Москва, 02-03 марта 2022 года. М.: Издательский дом Медиа Паблишер, 2022. С. 167-169. EDN AUXGNF

13. *Гадасин Д.В., Шведов А.В., Пантелеева К.А*. Предобработка информации для систем машинного обучения // Актуальные проблемы и перспективы развития экономики : Труды XXI Международной научно-практической конференции, Симферополь-Гурзуф, 20-22 октября 2022 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 268-269. EDN QVIOMF

14. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu*. Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60.

15. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю*. Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32.

16. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47.

17. *Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S*. Features of supporting decision making in modern enterprise infocommunication systems // T-Comm. 2019. Т. 13. № 3. С. 71-74.

18. *Гадасин Д.В., Кольцова А.В., Полякова А.Н*. Модель построения кластера для пограничных вычислений // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 86-92.

19. *Shvedov A.V., Gadasin D.V., Alyoshintsev A.V.* Segment routing in data transmission networks // T-Comm. 2022. Vol. 16. No. 5. P. 56-62. DOI 10.36724/2072-8735-2022-16-5-56-62. EDN VAYLJQ