Международный журнал информационных технологий и энергоэффективности

Том 9 Номер 5 (43)

2024

Международный журнал информационных технологий и энергоэффективности
Т.9 №5(43) 2024 г.

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Лихачев Н.И., Иванов Д.В. Сравнительный анализ технологий PON систем// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 5–12

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.77

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ PON СИСТЕМ

[1]Лихачев Н.И., [2]Иванов Д.В.

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФГБОУ ВО «МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ», Москва, Россия, (123423, г. Москва, ул. Народного Ополчения, 32), e-mail:[1]n.likhachev@inbox.ru, [2]Dima_19751975@mail.ru

В данной статье проводится сравнительный анализ PON сетей по таким техническим характеристикам как скорость, масштабируемость полоса пропускания нисходящего и восходящего потока. В статье будут рассмотрены такие технологии как G-PON,10G-PON, NG-PON2,25G-PON,50G-PON,100G-PON.

Ключевые слова**:** Технологии G-PON,10G-PON, NG-PON2,25G-PON,50G-PON,100G-PON.

COMPARATIVE ANALYSIS OF PON SYSTEMS TECHNOLOGIES

[1]Likhachev N.I., [2]Ivanov D.V.

ORDER OF THE RED BANNER OF LABOR OF THE MOSCOW TECHNICAL UNIVERSITY OF COMMUNICATIONS AND INFORMATICS, Moscow, Russia, (123423, Moscow, Narodnogo Opolcheniya str., 32), e-mail:[1]n.likhachev@inbox.ru, [2]Dima_19751975@mail.ru

This article provides a comparative analysis of PON networks based on such technical characteristics as speed, scalability, downstream and upstream bandwidth. The article will consider such technologies as G-PON,10G-PON, NG-PON2,25G-PON,50G-PON,100G-PON.

Keywords: G-PON, 10G-PON, NG-PON2, 25G-PON, 50G-PON, 100G-PON technologies.

Вашему вниманию предлагается статья на тему Сравнительный анализ технологий PON систем. Начать мы хотим с рассмотрения с самой распространенной технологии как G-PON. В данной статье будут рассмотрены такие технологии PON сетей как:

- G-PON - G.984 стандарт утвержден в 2003 году
- 10G-PON-(также известный XG-PON или G.987) утвержден в 2010 году Асимметрия.
- 10G-PON-(также известный XGS-PON, G.9807.1) утверждена 22.06. 2016 года. Симметрия.
- NG-PON2(также известная как TWDM-PON) утверждена в 2015 году.
- 25G PON технология.
- 50G PON. (также известная как HSP. G.9804.) утверждена в 2018 году.
- 100G PON технология.

Введение

Проблема, с которой приходится сталкиваться телекоммуникационным сетям – это в увеличении скорости доступа в предоставлении более широкой полосы пропускания.

Суть PON технологии заключается в создании полноценной пассивной оптической сети между OLT и ONT, с древовидной топологией, в промежуточных узлах находятся разветвители (сплиттеры) устройства, не требующие питания и технического обслуживания.

Технология GPON

настоящее время наиболее распространенной технологией является GPON пассивные оптические сети с гигабитной поддержкой, описанной в стандарте ITU-T G.984[1]

В GPON применяется технология WDM разделение каналов по длине волны, передаваемого по оптоволокну. Для загрузки данных используется длина волны 1490 нм, для оправки данных – 1310 нм [2.]**.**

10G-PON

Следующая технология, о которой мы хотели бы рассказать это технология 10G-PON (также известная как XG-PON или G.987) принятый стандарт 2010 года, где пропускная способность нисходящего канала 10 Гбит/с, а восходящего канала 2.5 Гбит/с соответственно. XG-PON является улучшенной версией GPON со значительно более расширенной полосой пропускания.

10GPON технологию еще называют XG-PON1 и XG-PON2 разница у них заключается только в поддерживаемых скоростях передачи. XG-PON1 именуемая еще как (XG-PON) пропускная способность передачи данных по нисходящему потоку 10Гбит/с и пропускная способность восходящего потока 2.5 Гбит/с, тогда как стандарт XG-PON2 именуемая еще как (XGS-PON) на симметричный нисходящий канал и восходящий канал 10 Гбит/с [3]. Аббревиатура S подчеркивает его симметричную архитектуру.

Длина волны в нисходящем направлении в технологии 10 GPON составляет 1577 нм, а соответственно восходящего направления составляет 1270 нм. Коэффициент деления если сравнивать с предыдущей технологией, которую мы рассматривали ранее у GPON он равнялся 1:64, а уже более новая 10 GPON поддерживает коэффициент разделения 1:128.

15 декабря 2023года компания «МТС» [4] объявила, что успешно провела свои тесты в городе Москве на магистральной сети фиксированного интернета XGS-PON поддерживающей скорость передачи данных до 10 Гбит/с, это во много раз превышает показатели нынешнего GPON. Успешное тестирование оборудования на узле связи подтвердило готовность компании МТС к подключению к сверхбыстрому интернету в 2024 году в квартиры в новых жилых комплексах г. Москвы только при наличии договоренности с застройщиками.

Что входит в тариф.

Тариф №8[5].

Выберите свою ультраскорость 40 Гбит/с 2500 мин.

Безлимитные соцсети и мессенджеры 200+ ТВ-каналов. Домашний интернет от 2 Гбит/с до 8 Гбит/с за 5990₽/мес.

Скорость в сети XGS-PON такова, что видеофайл с фильмом, сверхвысокой четкости объемом 8 Гб, загружаются за 20-25 секунд независимо от того сколько еще используется телефонов, планшетов и ноутбуков в квартире. Такая скорость актуальна для специалистов,

чьи профессии или увлечения связаны с ИТ-технологиями: видеомонтаж и звукорежиссура, строительство, обработка огромных данных, а также: игрокам или семьи, где используется большое количество телефонов, планшетов и ноутбуков.

Чтобы проверить как это все работает на узле связи в Москве было поставлено станционное оборудование XGS-PON OLT (Optical Line Terminal), а на стороне абонента испытали абонентское оборудование XGS PON ONT (Optical Network Terminal). Оборудование продемонстрировало бесперебойную и надежную работу со скоростью до 10 Гбит/с в восходящем и нисходящем потоках.

На международной выставке мобильной индустрии MWC 2024 компания D-Link анонсировала свою новую линейку оборудования с поддержкой технологии XGS-PON с доступом в интернет со скоростью до 10 Гбит/с, что в несколько раз превышает скорость актуальной на данной момент технологии GPON.

NG-PON2

Один из последних стандартов PON под эгидой ITU-T — стандарт NG-PON2 серии G.989 [6] стандарт, утвержденный в 2015 году.

Если XG-PON и XGS-PON — это одноканальные технологии, в которых предоставляемая полоса пропускания делится в соответствии с коэффициентом разделения, NG-PON2 — это многоканальная система PON, которая не только увеличивает пропускную способность волокна в четыре раза, но и предоставляет конфигурируемые оптические сетевые устройства (ONT), что дает значительное преимущество по сравнению с технологией 10G-PON.

Стандарт NG-PON2 обеспечивает общую пропускную способность сети 40Гбит/с в направлении DS и 10 Гбит/с в направлении US.

Такая скорость обеспечивается за счет использования нескольких длин волн с плотным разделением каналов по длине волны (DWDM) и технологии перестраиваемого приемопередатчика в абонентских терминалах (ONT).

Суть этой технологии (DWDM) заключается в том, что в одном волокне можно передавать несколько сигналов с разными длинами волн.

NG-PON2 использует выделенный диапазон длин волн: для направления DS выделяется диапазон от 1596 нм до 1602 нм, а для направления US выделяется диапазон от 1524 нм до 1544 нм.

Архитектура NG-PON2 обеспечивает мультиплексирование с временным разделением каналов (TWDM) и с разделением по длине волны. Мультиплексирование с разделением длины волны нисходящего потока происходит в результате объединения четырех OLT лазеров определенной длины волны с мультиплексированием длины волны. Потом свет проходя через фильтр находящийся в каждом ONT с помощью перестраиваемого фильтра, который пропускает к приемнику только определенную длину волны ниже по потоку. В направлении вверх по потоку перестраиваемым лазерам в каждом ONT динамически присваивается длина волны. Волокна от всех ONT объединены с пассивным мультиплексирующим устройством /разветвителем. Мультиплексирование с временным разделением данных обеспечивается в направлении вверх по потоку за счет использования импульсных лазеров в каждом ONT.

Благодаря мультиплексированию с разделением по длине волы на четырех длинах волн, с полосой пропускания в 10 Гбит /с каждая, NG-PON2 может организовать пропускную способность до 40 Гбит/с.

Преимущество этого решения является возможность то, что оптические каналы могут быть зарезервированы для ONT. В базовой конфигурации восемь каналов PtP WDM обеспечивают сочетания со старыми PON системами.

Топологии следующего поколения 25G-PON

В отличие от китайских компаний, специализирующихся на телекоммуникационном оборудовании которые выбрали технологию 50G PON оборудовании европейские компании пошли в сторону технологии 25G PON.

Компания Nokia 12 марта 2024 г анонсировала симметричный оптоволоконный модем 25G PON (модель U-010Y-A)[7], предназначенный для создания сетей связи с высокой пропускной способностью. У модема поддерживается симметричная пропускная способность 25 Гбит/с.

По заявлениям компании Nokia, новое решение 25G PON позволяет операторам модернизировать существующую сеть GPON или XGS PON для обеспечения скорости 10 Гбит/с и более.

Модем может применятся для подключения сотовых станций и для передачи мобильного трафика по PON сети в режиме plug-and-play. Для него заявлена возможность работать вместе с такими технологиями как с GPON, XGS-PON и 50G PON.

На сегодняшний день Nokia поставила более 1 млн портов 25G PON. Технологию внедряют такие компании, как Google Fiber, EPB, Vodafone Qatar и OGI. Более 30 операторов по всему миру тестируют 25G PON для различных сценариев использования.

Топологии для следующего поколения 50G-PON

50G-PON — это технология, позволяющая передавать данные со скоростью 50GГбит/с на одной длине волны.

23 апреля 2021 года был введен международный стандарт 50G PON который официально был принят на общем собрании 15-й исследовательской группы Международного союза электросвязи (ITU-T SG15). 50G TDM PON — это технология PON нового поколения после 10G PON. 50G PON уже был запущен в коммерческое использование в 2023 году в Европе.

G.9804.3[8] (G.hsp.50Gpmd): спецификация пассивных оптических сетей с поддержкой 50 гигабит (50G-PON) – спецификация уровня зависимости от физических носителей (PMD) – это стандарт для жилых коммерческих и мобильных сетей. Этот стандарт был утвержден в сентябре 2021 года. В сентябре 2021 года ITU-T официально представил первую версию стандарта 50G-PON. Она включает технические спецификации, которые поддерживают асимметричные скорости и сосуществование двух поколений (10G-PON или GPON).

Усовершенствованные варианты взаимодействуют между собой и поддерживают плавное обновление, при этом методы реализации разделены на две схемы: двухрежимную MPM (встроенный компонент объединения волн) и внешнее объединение волн.

Поставщик, который активно вкладывает деньги в индустриализацию сети 50G-PON и постоянно продвигает ее вперед это компания ZTE.

100G PON технология

100G-PON — это технология широкополосного доступа, разработанная компанией FiberHome.

Она предоставляет скорость 25 Гбит/с на одной длине волны и является наиболее перспективной в данной области.

Пропускная способность одного волокна может достигать 100Гбит/с обеспечивая гигабитный широкополосный доступ для конечных пользователей, а также удовлетворяя требованиям сотовых сетей пятого поколения со скоростью доступа до 10 Гбит/с.

Технология 100G-PON разрабатывается в сотрудничестве с организациями по стандартизации IEEE/FSAN/ITU-T.

В заключении я хотел бы подвести итоги всего вышесказанного и выразить это в таблице.

Таблица 1 – Сравнительная характеристика PON сетей.

	G-PON	XG-PON	XGS-PON	NG-PON2	25G-PON	50G-PON
Стандарт	G.984	G.987	G.9807.1	G.989	25G-PON	G.9804(HSP)
Полоса пропускания вниз по потоку	2.5Гбит/с	10Гбит/с	10Гбит/с	40Гбит/с	25Гбит/с	50Гбит/с
Полоса пропускания вверх по потоку	1.25Гбит/с	2.5Гбит/с	10Гбит/с	10Гбит/с	10/25Гбит/с	10/25/50Гбит/с
Масштабируемость	1:64	1:128	1:128	1:256	1:512	1:512
Год	2003г.	2010г.	2016г.	2015г.		2021г.
Макс. длина передачи, км	60	100	100	100	–	
Длина волны прямой поток	1490нм	1577нм	1577нм	1596-1602		
Длина волны обратный поток	1310нм	1270нм	1270нм	1524-1544		

Технические характеристики 100G PON

Факторы, которые следует учитывать при выборе длин волн для PON 100G, включают дисперсию волокна, потери в волокне, совместимость с PON, стоимость оптических устройств и техническую сложность. 100G PON поддерживает три скорости: 25G, 50G и 100G. ZTE в союзе с несколькими компаниями отрасли предлагает план использования всех длин волн O-диапазона, который был принят организациями по стандартизации. Схема длины волны имеет много преимуществ, таких как модуляция NRZ, отсутствие сложной компенсации дисперсии, использование лазеров с прямой модуляцией (DMLs) и лазеров с внешней модуляцией (eMLS), а также простота реализации на физическом уровне.

Технические характеристики 25G PON

Увеличение пропускной способности в 2,5 раза при увеличении затрат менее чем в 2,5 раза является экономически эффективной стратегией. Для этого можно использовать длины волн O-диапазона, упрощенную передачу данных с использованием технологий центров обработки данных (NRZ), по сравнению со сложными и дорогостоящими схемами модуляции, такими как PAM4, снижение энергопотребления и двухскоростную передачу данных на 5 дБ до 25 Гбит / с по сравнению с 10 Гбит / с за счет сочетания более высокой мощности запуска, повышенной чувствительности приемника и надежного FEC позволяет придерживаться бюджета потерь на 29 дБ.

Стандарт 25G-PON предписывает использование длины волны 1358 нм для нисходящего потока и предоставляет три варианта нисходящего потока.

- **Вариант 1:** 1300 нм (подмножество GPON) для совместной работы с XGS-PON.
- **Вариант 2:** 1270 нм (такой же, как у XGS-PON) для совместной работы с GPON.
- **Вариант 3:** 1286 нм для поддержания тройного взаимодействия с 25G PON, XGS-PON и GPON.

Технические характеристики 50G-PON

Эти данные включают в себя использование длины волны 1340-1344 нм для нисходящего потока и дают три варианта нисходящего потока.

- *Вариант 1: 1260-1280 нм широкополосный для совместной работы с GPON*
- *Вариант 2: 1290-1310 нм широкополосный для совместной работы XGS-PON и XG-PON*
- *Вариант 3: 1298-1302 нм узкополосный для обеспечения тройного взаимодействия 25G PON.*

Технические характеристики 100G PON

При выборе длин волн для PON 100G следует учитывать дисперсию волокна, потери в волокне, совместимость с PON, стоимость оптических устройств и техническую сложность. 100G PON поддерживает три скорости: 25G, 50G и 100G.

ZTE предлагает использование всех длин волн O-диапазона, что имеет много преимуществ, таких как модуляция NRZ, отсутствие сложной компенсации дисперсии и простота реализации на физическом уровне.

Технология PON продолжает развиваться, чтобы соответствовать требованиям к высокоскоростному и эффективному широкополосному доступу. GPON, XG PON и XGS PON предлагают разные скорости и полосы пропускания. NG-PON2 является многоканальной системой PON, которая увеличивает пропускную способность волокна и предоставляет конфигурируемые оптические сетевые устройства.

С каждой последующей технологией (25G PON, 50G PON, 100G PON) увеличивается полоса пропускания и скорость интернета.

Заключение

Технология PON продолжает развиваться, чтобы соответствовать требованиям к высокоскоростному и эффективному широкополосному доступу. GPON, XG PON и XGS PON

предлагают разные скорости и полосы пропускания. NG-PON2 является многоканальной системой PON, которая увеличивает пропускную способность волокна и предоставляет конфигурируемые оптические сетевые устройства.

С каждой последующей технологией (25G PON, 50G PON, 100G PON) увеличивается полоса пропускания и скорость интернета.

Список литературы

1. ITU-T Recommendation G.984.1: Пассивные оптические сети с поддержкой гигабита (GPON): общие характеристики". ITU-T. 2003-2012.
2. Салтыков. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 128 с. — Текст: электронный //Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/180158 (дата обращения: 19.03.2024).
3. ITU-T Recommendation "Пассивные оптические сети с поддержкой 10 гигабит (XG-PON): общие требования". G.987. Международный союз электросвязи. 13 января 2010 г. Проверено 7 мая 2011 года.
4. МТС запустит технологию XGS-PON для сверхскоростного домашнего интернета Электронный ресурс. URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2023-12-15/mts-zapustit-tehnologiyu-xgs-pon-dlya-sverhskorostnogo-domashnego-interneta (дата обращения 21.03.2024 года).
5. Ультраскорость вашего домашнего интернета. Электронный ресурс. URL: https://x.mts.ru/xgspon
6. Электронный ресурс. URL: ITU-T Recommendation G.989.2 https://www.itu.int/rec/T-REC-G.989.2. 3
7. Электронный ресурс. Nokia запускает новый оптоволоконный модем 25G PON для ускорения развертывания многогигабитной широкополосной связи. URL: https://www.nokia.com/about-us/news/releases/2024/03/12/nokia-launches-new-25g-pon-fiber-modem-to-accelerate-multi-gigabit-broadband-deployments/(дата обращения 21.03.2024 года).
8. Электронный ресурс. URL: ITU-T Recommendation G.9804. (G.hsp.50Gpmd) – https://en.everybodywiki.com/50-Gigabit-capable_passive_optical_networks ".

References

1. ITU-T Recommendation G.984.1: Passive optical networks with Gigabit support (GPON): general characteristics". ITU-T. 2003-2012.
2. Saltykov. — St. Petersburg: St. Petersburg State University named after M.A. Bonch-Bruevich, 2019. — 128 p. — Text: electronic // Lan: electronic library system. — URL: https://e.lanbook.com/book/180158 (date of reference: 03/19/2024).
3. ITU-T Recommendation "10 Gigabit passive optical networks (XG-PON): general requirements". G.987. International Telecommunication Union. January 13, 2010 Verified on May 7, 2011.
4. MTS will launch XGS-PON technology for ultra-high-speed home Internet Electronic resource. URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2023-12-15/mts-zapustit-tehnologiyu-xgs-pon-dlya-sverhskorostnogo-domashnego-interneta (accessed 03/21/2024).

5. Ultra-speed of your home Internet connection. An electronic resource. URL: https://x.mts.ru/xgspon
6. Electronic resource. URL: ITU-T Recommendation G.989.2 https://www.itu.int/rec/T-REC-G.989.2. 3
7. Electronic resource. Nokia is launching a new 25G PON fiber modem to accelerate the deployment of multi-gigabit broadband. URL: https://www.nokia.com/about-us/news/releases/2024/03/12/nokia-launches-new-25g-pon-fiber-modem-to-accelerate-multi-gigabit-broadband-deployments/(accessed 03/21/2024).
8. Electronic resource. URL: ITU-T Recommendation G.9804. (G.hsp.50Gpmd) – https://en.everybodywiki.com/50-Gigabit-capable_passive_optical_networks ".

Огольцова Н.Д. Использование метода TF-IDF для детектирования вредоносных PDF файлов // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 13–17

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИСПОЛЬЗОВАНИЕ МЕТОДА TF-IDF ДЛЯ ДЕТЕКТИРОВАНИЯ ВРЕДОНОСНЫХ PDF ФАЙЛОВ

Огольцова Н.Д.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: og.nata@inbox.ru

В статье рассматривается применение метода TF-IDF (Term Frequency-Inverse Document Frequency) для обнаружения вредоносных PDF файлов. Исследуется, как этот метод может быть использован для анализа текста внутри PDF документов, чтобы определить, содержит ли файл вредоносный код или нет. Метод TF-IDF позволяет извлекать ключевые слова из текста, что делает его эффективным инструментом для анализа больших объемов данных. В статье подробно описывается процесс интеграции TF-IDF с алгоритмами машинного обучения, что позволяет значительно улучшить точность и эффективность обнаружения вредоносных файлов. Также рассматриваются преимущества и ограничения предложенного подхода, а также возможности интеграции с другими извлекаемыми признаками из PDF документов для детектирования их вредоносности.

Ключевые слова: TF-IDF, PDF, машинное обучение, классификация документов, извлечение признаков.

USING THE TF-IDF METHOD TO DETECT HARMFUL PDF FILES

Ogoltsova N.D.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: og.nata@inbox.ru

The article discusses the application of the TF-IDF (Term Frequency-Inverse Document Frequency) method for detecting malicious PDF files. We are investigating how this method can be used to analyze text inside PDF documents to determine whether a file contains malicious code or not. The TF-IDF method allows you to extract keywords from text, which makes it an effective tool for analyzing large amounts of data. The article describes in detail the process of integrating TF-IDF with machine learning algorithms, which significantly improves the accuracy and efficiency of detecting malicious files. The advantages and limitations of the proposed approach are also considered, as well as the possibility of integration with other extracted features from PDF documents to detect their harmfulness.

Keywords: TF-IDF, PDF, machine learning, document classification, feature extraction.

PDF (Portable Document Format) — это формат документа, разработанный компанией Adobe Systems в 1990-х годах. Цель создания формата PDF заключалась в создании стандарта для представления документов и других справочных материалов в формате, который не зависит от прикладного программного обеспечения, аппаратного обеспечения и операционной системы. PDF может содержать текст, изображения, гиперссылки, поля форм, мультимедийные материалы, цифровые подписи, вложения, метаданные, геопространственные функции и 3D-объекты. Формат PDF широко используется для обмена

информационными данными между пользователями, так как поддерживается большинством операционных систем, мобильной и компьютерной техники. [1]

По данным подразделения Netskope Threat Labs Stats, американской софтверной компании NetScope, основанной в 2012 году, за ноябрь 2023, формат PDF документа является самым часто используемым форматов для использования в киберпреступности.

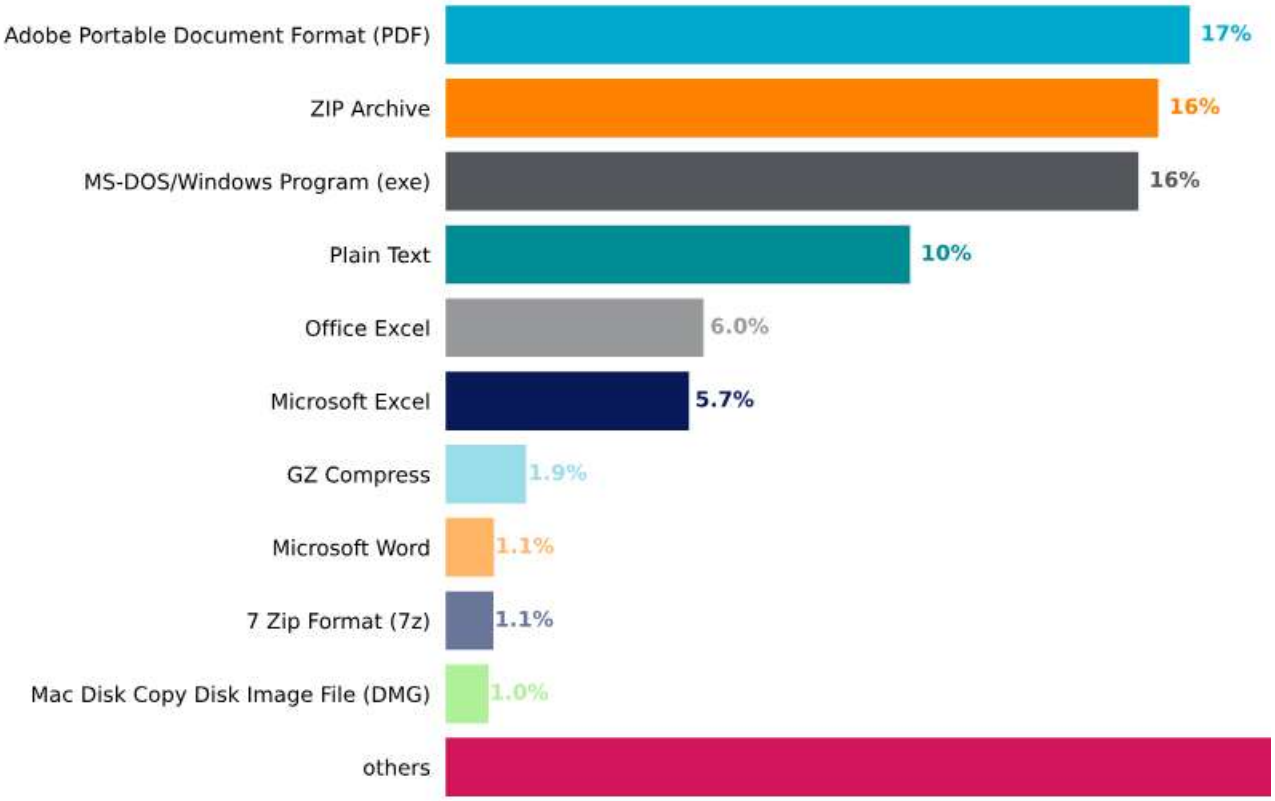

Рисунок 1 – Топ форматов документов по использованию в киберпреступлениях

Согласно статистике, почти половина всех атак вредоносного ПО направлена на малые предприятия, делая их основной мишенью для атак вредоносного ПО. Большинство малых предприятий плохо подготовлены к отражению таких атак, поскольку они обычно не имеют специализированных ИТ-специалистов или надежных систем безопасности. [2]

Вредоносные PDF-файлы могут быть распространены через различные каналы, включая электронную почту, веб-сайты и социальные сети. Киберпреступники могут использовать различные тактики, включая поддельные профили, вредоносные ссылки и обманчивую рекламу, чтобы заставить пользователей скачать или открыть эти файлы.

Методы детектирования вредоносных PDF файлов включают в себя два основных метода – это динамический и статический анализ.

Динамический анализ подразумевает использование поведенческого анализатора для обнаружения аномалий в поведении вредоносных PDF файлов, таких как попытки выполнения вредоносного кода или попытки эксплуатации уязвимостей в программном обеспечении. Этот метод использует инструменты для мониторинга поведения программы в реальном времени, чтобы выявить ошибки, уязвимости и проблемы, которые могут возникнуть только при выполнении программы.

Статический анализ нацелен на поиск известных сигнатур вредоносного кода внутри PDF файлов. Это может включать в себя поиск уникальных хешей вредоносных файлов, которые были обнаружены и анализированы в прошлом. К этому методу также относится и анализ вредоносного JavaScript в PDF файлах, спрятанного в объектах и дешифруемого другим JavaScript кодом, для обнаружения и анализа вредоносного кода.

Преимуществом динамического анализа является возможность обнаружить ошибки и уязвимости, которые возникают только при выполнении программы или открытия файла, однако он может быть более трудоемким и затратным по времени, чем статический анализ, особенно для больших и сложных программ. Статический анализ не требует большого затрата ресурсов, но он подразумевает наличие большой базы исходных данных для точного детектирования. [3]

Исходя из приведённой информации, самым лёгким для последующего внедрения и использования, является статический метод. Используя при этом методы машинного обучения, можно получить модель, способную детектировать вредоносные PDF файлы с высокой точностью.

В исследовании AlMahadeen Awss и Alkasassbeh Mouhammd «PDF Malware Detection using Machine learning» от 2023 года приведён эксперимент, в котором извлекаются сигнатурные признаки из PDF документов, общим количеством – 32, и в последующем обучаются на алгоритме случайного леса в соотношении 80:20. В своём исследовании авторы смогли получить значения точности модели равное 99.5%. [4]

Метод TF-IDF (Term Frequency-Inverse Document Frequency) может улучшить показатель точности — это статистическая мера, которая оценивает, насколько слово релевантно для документа в коллекции документов. Это достигается путем умножения двух метрик: частоты появления слова в документе и обратной частоты документа (IDF) слова в наборе документов.

Частота термина (Term Frequency, TF) определяет, сколько раз слово появляется в документе. Чем чаще слово встречается в документе, тем выше его значение TF.

TF-IDF используется в автоматизированном текстовом анализе и очень полезен для оценки слов в алгоритмах машинного обучения для обработки естественного языка (NLP). Он был изобретен для поиска документов и извлечения информации и работает, увеличиваясь пропорционально количеству раз, когда слово появляется в документе, но компенсируется количеством документов, содержащих это слово.

Пример использования TF-IDF в Python может включать использование метода TfidfVectorizer() из модуля sklearn.feature_extraction.text, который позволяет вычислять значения TF-IDF для слов в документах. [5]

Однако, стоит отметить, что TF-IDF имеет свои ограничения, такие как проблемы с очень редкими терминами, отсутствие понимания смысла или контекста слов, игнорирование порядка слов и трудности с интерпретацией синонимов и похожих слов. [6]

Создание модели, обученной на признаках, извлеченных с помощью парсера PDF файлов, и словах, обработанных с использованием TF-IDF, представляет собой инновационный подход к анализу и классификации PDF документов, особенно в контексте обнаружения вредоносного содержимого. Данная модель может быть внедрена в уже существующие ресурсы, например, почтовые сервисы, для анализа и обнаружения вредоносных файлов.

Этот подход может можно считать наиболее эффективным для обнаружения вредоносных PDF файлов, так как он сочетает в себе анализ структуры файла и анализ текстового содержимого, что позволяет модели лучше понимать характеристики вредоносных документов.

В заключении, объединение этих двух методов в процессе обучения модели машинного обучения может значительно улучшить ее способность к точному обнаружению вредоносных PDF файлов. Этот подход может быть особенно полезен для исследователей в области безопасности информации, специалистов по кибербезопасности и разработчиков ПО, работающих над обнаружением и предотвращением вредоносного ПО. Этот подход можно считать эффективным и многоаспектным к обнаружению вредоносных PDF файлов. Он может служить основой для разработки более продвинутых систем обнаружения вредоносного ПО, способных адаптироваться к новым угрозам и методам атаки.

Список литературы

1. «Обзор формата PDF» [Электронный ресурс] URL: https://helpx.adobe.com/ru/incopy/using/pdf.html (Дата обращения: 27.03.2024);
2. «Актуальные киберугрозы: III квартал 2023 года» [Электронной ресурс] URL: https://www.netskope.com/blog/netskope-threat-labs-stats-for-september-2023 (Дата обращения: 27.12.2023);
3. Li, Min & Zhou, Ying & Yu, Min & Liu, Chao. (2016). Combining static and dynamic analysis for the detection of malicious JavaScript-bearing PDF documents. 475-482. 10.1142/9789813200449_0059. (Дата обращения: 27.03.2024);
4. AlMahadeen, Awss & Alkasassbeh, Mouhammd. (2023). PDF Malware Detection using Machine learning. 10.20944/preprints202301.0557.v1 (Дата обращения: 27.03.2024);
5. «Understanding TF-IDF (Term Frequency-Inverse Document Frequency)» [Электронный ресурс] URL: https://www.geeksforgeeks.org/understanding-tf-idf-term-frequency-inverse-document-frequency/ (Дата обращения: 27.03.2024);
6. Jayady, Siti & Antong, Hasmawati. (2021). Theme Identification using Machine Learning Techniques. Journal of Integrated and Advanced Engineering (JIAE). 1. 123-134. 10.51662/jiae.v1i2.24. (Дата обращения: 27.03.2024).

References

1. «Overview of the PDF format.» [Web resource] URL: https://helpx.adobe.com/ru/incopy/using/pdf.html (Date of address: 27.03.2024);
2. «Current cyber threats: third quarter 2023» [Web resource] URL: https://www.netskope.com/blog/netskope-threat-labs-stats-for-september-2023 (Date of address: 27.12.2023);
3. Li, Min & Zhou, Ying & Yu, Min & Liu, Chao. (2016). Combining static and dynamic analysis for the detection of malicious JavaScript-bearing PDF documents. 475-482. 10.1142/9789813200449_0059. (Date of address: 27.03.2024);
4. AlMahadeen, Awss & Alkasassbeh, Mouhammd. (2023). PDF Malware Detection using Machine learning. 10.20944/preprints202301.0557.v1 (Date of address: 27.03.2024);

5. «Understanding TF-IDF (Term Frequency-Inverse Document Frequency)» [Web resource] URL: https://www.geeksforgeeks.org/understanding-tf-idf-term-frequency-inverse-document-frequency/ (Date of address: 27.03.2024);
6. Jayady, Siti & Antong, Hasmawati. (2021). Theme Identification using Machine Learning Techniques. Journal of Integrated and Advanced Engineering (JIAE). 1. 123-134. 10.51662/jiae.v1i2.24. (Date of address: 27.03.2024).

Удальцов К.Р. Кибербезопасность в здравоохранении: стратегии защиты медицинских данных и оборудования// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 18–22

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ: СТРАТЕГИИ ЗАЩИТЫ МЕДИЦИНСКИХ ДАННЫХ И ОБОРУДОВАНИЯ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья обсуждает важность кибербезопасности в здравоохранении и стратегии защиты медицинских данных и оборудования от киберугроз. В контексте цифровизации здравоохранения и увеличения угроз кибератак, обеспечение безопасности медицинских информационных систем становится критически важным для сохранности данных пациентов и непрерывности медицинского ухода. Статья охватывает рост угроз, защиту медицинских данных, безопасность медицинского оборудования, развитие стратегий кибербезопасности, будущие вызовы и важность сотрудничества между стейкхолдерами. Она подчеркивает необходимость инвестирования в кибербезопасность, обучения персонала, соблюдения законодательства и принятия инновационных решений для обеспечения безопасности и надежности здравоохранения в эпоху цифровой трансформации.

Ключевые слова: Кибербезопасность, здравоохранение, медицинские данные, медицинское оборудование, киберугрозы, защита данных, кризисное управление, обучение персонала, законодательство, сотрудничество, инновации, безопасность пациентов, цифровизация, угрозы, стратегии защиты.

CYBERSECURITY IN HEALTHCARE: STRATEGIES FOR PROTECTING MEDICAL DATA AND EQUIPMENT

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance of cybersecurity in healthcare and strategies for protecting medical data and equipment from cyber threats. In the context of digitalization of healthcare and increasing threats of cyber attacks, ensuring the security of medical information systems is becoming critically important for the safety of patient data and continuity of medical care. The article covers the growth of threats, the protection of medical data, the security of medical equipment, the development of cybersecurity strategies, future challenges and the importance of cooperation between stakeholders. She emphasizes the need to invest in cybersecurity, train staff, comply with legislation, and make innovative decisions to ensure the safety and reliability of healthcare in an era of digital transformation.

Keywords: Cybersecurity, healthcare, medical data, medical equipment, cyber threats, data protection, crisis management, staff training, legislation, cooperation, innovation, patient safety, digitalization, threats, protection strategies.

Введение

В эпоху цифровизации здравоохранения, когда медицинские данные переносятся в онлайн-среду и медицинское оборудование становится все более сетевым, вопрос кибербезопасности становится жизненно важным. [1] Защита медицинских данных и оборудования от киберугроз становится приоритетом для обеспечения непрерывности медицинского ухода и предотвращения возможных угроз для пациентов и организаций здравоохранения.

1. **Рост угроз в здравоохранении:**

С каждым годом случаи кибератак на медицинские учреждения увеличиваются. Злоумышленники могут нацелиться на медицинские данные пациентов, шантажировать организации здравоохранения или даже нарушить работу медицинского оборудования. [2] Это создает серьезные угрозы как для конфиденциальности данных, так и для безопасности пациентов.

2. **Защита медицинских данных:**

Одним из ключевых аспектов кибербезопасности в здравоохранении является защита медицинских данных. [3] Организации должны строго соблюдать нормы безопасности, шифровать данные, устанавливать системы мониторинга и обучать персоналу правилам работы с конфиденциальной информацией.

3. **Безопасность медицинского оборудования:**

С развитием Интернета вещей (IoT) медицинское оборудование становится более уязвимым для кибератак. [4] Взлом медицинских устройств может привести к серьезным последствиям, включая неправильное лечение пациентов. Производители медицинского оборудования должны уделять особое внимание кибербезопасности, внедряя защитные механизмы и обновления.

4. **Развитие стратегий кибербезопасности:**

Для эффективной защиты медицинских данных и оборудования необходимо разработать комплексные стратегии кибербезопасности. [5] Это включает в себя постоянное обновление систем безопасности, обучение персонала, аудит безопасности и сотрудничество с киберспециалистами.

5. **Будущее кибербезопасности в здравоохранении:**

С увеличением объема медицинских данных, использованием искусственного интеллекта в медицине и расширением интернета вещей, вопросы кибербезопасности станут только более актуальными. [6] В будущем необходимо ожидать новых вызовов, таких как квантовые вычисления и биометрическая аутентификация, которые потребуют новых стратегий защиты.

6. **Важность сотрудничества и обмена информацией:**

Для эффективной борьбы с киберугрозами в здравоохранении необходимо усилить сотрудничество между медицинскими учреждениями, государственными органами, киберспециалистами и производителями медицинского оборудования. Обмен опытом и информацией поможет создать более устойчивые системы защиты.[7]

7. Подготовка персонала:

Одним из ключевых моментов в обеспечении кибербезопасности в здравоохранении является обучение персонала. Все сотрудники медицинских учреждений должны быть осведомлены о рисках кибератак и знать основные правила безопасности, чтобы минимизировать уязвимости систем.

8. Регулирование и законодательство:

Законы и нормативные акты в области кибербезопасности играют важную роль в защите медицинских данных. [8] Государства должны разрабатывать строгие правила и стандарты для организаций здравоохранения и производителей медицинского оборудования, чтобы обеспечить соответствие требованиям безопасности.

9. Кризисное управление:

Подготовка к кибератакам и разработка планов кризисного управления являются неотъемлемой частью стратегии кибербезопасности в здравоохранении. Организации должны иметь четкие инструкции по реагированию на инциденты безопасности, включая изоляцию уязвимостей, восстановление данных и устранение угроз.

10. Обучение пациентов:

Важным аспектом обеспечения кибербезопасности в здравоохранении является обучение пациентов основам безопасности данных. Пациентам следует быть осведомленными о рисках киберугроз и методах защиты своих медицинских данных, чтобы предотвратить возможные атаки на их личную информацию.

11. Инновации в области кибербезопасности:

Развитие новых технологий, таких как блокчейн и квантовые вычисления, открывает новые возможности для улучшения кибербезопасности в здравоохранении. Интеграция инновационных решений может повысить защиту медицинских данных и оборудования, делая системы более надежными и устойчивыми к угрозам.

Заключение

Кибербезопасность в области здравоохранения остается одним из наиболее актуальных и важных вопросов в современном мире. Защита медицинских данных и оборудования требует комплексного подхода, включающего в себя технологические инновации, сотрудничество между стейкхолдерами, обучение персонала и пациентов, а также строгое соблюдение законодательства. Только совместными усилиями можно обеспечить безопасность и надежность здравоохранения в цифровой эпохе.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.

8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Капитанчук В.В., Трофимов П.С. Моделирование процесса устранения нарушений регулярности полетов в сбойных ситуациях // Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 23–32

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.94

МОДЕЛИРОВАНИЕ ПРОЦЕССА УСТРАНЕНИЯ НАРУШЕНИЙ РЕГУЛЯРНОСТИ ПОЛЕТОВ В СБОЙНЫХ СИТУАЦИЯХ

Капитанчук В.В., [1]Трофимов П.С.
ФГБОУ ВО "УЛЬЯНОВСКИЙ ИНСТИТУТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ Б.П. БУГАЕВА", Ульяновск, Россия (432071, Ульяновская область, г. Ульяновск, ул. Можайского, зд 8/8), e-mail: [1]pashaveles1337@gmail.com

В данной научной статье представлена модель алгоритма устранения нарушений регулярности полетов в сбойных ситуациях. Рассматривается анализ основных причины нарушений, разрабатываются методы оптимизации процессов оперативного управления аэропортом и предложения по решению для минимизации негативных последствий.

Ключевые слова: Регулярность полетов, сбойные ситуации, алгоритм, оптимизация, авиаперевозки.

MODELING THE PROCESS OF ELIMINATING VIOLATIONS OF FLIGHT REGULARITY IN EMERGENCY SITUATIONS

Kapitanchuk V.V., [1]Trofimov P.S.
ULYANOVSK INSTITUTE OF CIVIL AVIATION NAMED AFTER CHIEF MARSHAL B.P. BUGAEV, Ulyanovsk, Russia (432071, Ulyanovsk region, Ulyanovsk, Mozhaisky str., zd 8/8), e-mail: [1]pashaveles1337@gmail.com

This scientific article presents a model of an algorithm for eliminating violations of flight regularity in emergency situations. The analysis of the main causes of violations is considered, methods for optimizing the processes of operational management of the airport and proposals for solutions to minimize negative consequences are being developed.

Keywords: Flight regularity, disruptive situations, algorithm, optimization, air transportation.

Введение.

Определение проблемы

В современном мире авиационная отрасль играет важную роль в обеспечении глобальной связности, экономического роста и машиностроения. Однако, эффективность авиационной отрасли во многом зависит от регулярности полетов, которая может быть нарушена из-за различных сбойных ситуаций. Эти сбои могут привести к задержкам и отменам рейсов, что негативно сказывается на уровне удовлетворенности пассажиров и экономической эффективности авиакомпаний. [3]

Решение этой проблемы требует комплексного подхода, включая применение современных технологий и автоматизированных систем управления. С использованием передовых технологий, таких как искусственный интеллект, анализ данных и

автоматизированные алгоритмы принятия решений, эти системы способны предсказывать возможные нарушения, а также быстро реагировать на изменяющиеся условия.

Цель и задачи исследования, методология исследования

В этой статье представляется модель алгоритма корректирующих действий по устранению нарушений регулярности полетов в сбойных ситуациях. Наша цель - анализировать основные причины нарушений, разрабатывать методы оптимизации процессов оперативного управления аэропортом и предлагать решения для минимизации негативных последствий.

Данная работа начинается с обзора существующих исследований в области регулярности полетов и сбойных ситуаций. Затем идет анализ основных причин нарушений и их влияние на операции аэропорта. На основе этого анализа разрабатывается алгоритм устранения нарушений и оценка его эффективности.

Данные исследования должны помочь улучшить уровень регулярности полетов и увеличить эффективность операций аэропорта.

1. Анализ нарушений регулярности отправления воздушных судов, приводящих к сбойным ситуациям, и их влияния на показатели эффективности аэропорта

Аэропорт представляет собой интегрированный комплекс, включающий в себя аэродром, терминалы и прочие здания, созданные для обеспечения взлёта и посадки самолётов, а также сервиса авиаперевозок, оснащённые всем необходимым оборудованием, квалифицированным авиационным и вспомогательным персоналом. Основные задачи, которые выполняет аэропорт в рамках своей производственной деятельности и которые сосредоточены вокруг обслуживания, чётко прописаны в директивах Международной организации гражданской авиации (ICAO). [2]

Пунктуальность авиарейсов отражает эффективность работы авиакомпаний и местных органов управления гражданской авиацией (ТУГА – территориальных управлений гражданской авиации), а также их способность доставлять пассажиров, багаж и грузы в соответствии с условиями транспортного соглашения.

Процентная оценка регулярности отправления рейсов вычисляется как соотношение своевременно отправленных самолетов к общему числу запланированных отправлений, при этом задержка считается, если самолет покидает аэропорт позже утвержденного времени вылета. Кроме того, регулярность полетов оценивается по таким параметрам, как точность посадки, прибытия, отправления и вылета рейсов. [1]

Выход рейса считается регулярным, если:

- взлет был произведен не позднее расчетного времени взлета;
- взлет позже расчетного времени, но в первой точке посадки на траекторию полета судна произошедшее в установленное время по плану полета.

Регулярность отправления вооруженных сил тесно связана с работой аэропортов, состояние которых определяется следующими ситуациями:

- штатная ситуация;
- нештатная ситуация;
- сбойная ситуация.

Штатная ситуация в аэропорту подразумевает его функционирование и всех входящих в его состав служб в соответствии с заранее разработанным планом полетов, основанным на утвержденном расписании. В случае возникновения нестандартных условий, когда деятельность аэропорта происходит с отклонениями от стандартного процесса из-за ограниченных ресурсов или введения дополнительных рейсов, это не приводит к остановке его работы, но требует незамедлительных действий по корректировке и усиленного контроля над всеми службами для обеспечения соответствия установленным стандартам. [4]

Сбойная ситуация в аэропорту возникает при серьезных нарушениях стандартных процедур, что приводит к скоплению пассажиров. Такие сбои могут быть вызваны закрытием аэропортов назначения, для которых аэропорт отправления является запасным, или задержками рейсов из-за закрытия аэропорта отправления. С точки зрения авиакомпаний, причиной сбоя является любая ситуация, которая неожиданно ухудшает условия перевозки и нарушает обязательства компании по обеспечению качества услуг.

Аварийные ситуации часто связаны с форс-мажорными обстоятельствами, которые возникают вне зависимости от действий аэропорта или авиакомпании и которые невозможно предвидеть или предотвратить. К таким обстоятельствам относятся, например, экстремальные погодные условия, социальные беспорядки, террористические акты, временные ограничения, связанные с проведением официальных мероприятий, технические неисправности, нехватка парковочных мест, инциденты на взлетно-посадочной полосе и другие.

Иногда сбои могут быть спровоцированы недостатками в координации между службами, ответственными за управление чрезвычайными ситуациями, а также системными недочетами в работе отдельных подразделений, недостаточной реализацией существующих процедур и т.д. Для устранения последствий сбоев предпринимаются оперативные меры, включающие корректировку стандартных процедур и порядка обслуживания воздушных судов на земле. В классификаторе нарушений регулярности полетов выделены основные причины, влияющие на возникновение аварийных ситуаций в аэропорту, и определены ответственные за них стороны, включая аэропорт, авиакомпании и другие организации. [4],[5]

Таблица 1 – Выборка из классификатора нарушений регулярности полетов ВСГА значимых нарушений, наиболее влияющих на возникновение сбойных ситуаций по вине служб аэропорта, авиаперевозчиков и других факторов [1]

Код	Служба	Нарушения
И	ИАС	И05. Ошибки в планировании ТО, приведшие к необеспечению СПП. И13. Авиационное происшествие или инциденты по вине службы.
П	СОП	П13. Отказ пассажиров от полета после окончания посадки. П22. Несвоевременное внесение изменений в расписание.
Б	Служба бортпроводников	Б01. Опоздание на вылет в базовом, промежуточном и конечномаэропортах, в том числе из-за отсутствия резерва бригад бортпроводников.
Ш	Служба главного механика	Ш03. Отказы и неисправности стационарных и подвижных внутриаэропортовых средств механизации, спецоборудования.

А	Аэродромнаяслужба	А03. Внеплановый ремонт ВПП, РД, МС и перронов. А04. Повреждение ВС и наземных светотехнических средств повине служб. А05. Невыдерживание установленных плановых сроков ремонтаэлементов летного поля по вине аэродромной службы.
Г.	Служба ГСМ	Г01. Отказы и неисправности в работе стационарных средств заправки и перекачки топлива. Г04. Несвоевременное обеспечение поставок ГСМ. Г05. Несвоевременная доставка (перекачка) ГСМ от прирельсового или берегового склада ГСМ аэропорта до емкостей расходного склада или системы централизованной заправки ВС топливом. Г06. Подача на заправку некондиционных ГСМ и спецжидкостей.
Л	Летная служба	Л13. Эвакуация ВС с летного поля, если его занятость произошла по вине летного экипажа.
Д	Служба движения	Д04. Несогласованное с ПДС принятие решения на прием ВС или планирование ВС на вылет без учета пропускной способности аэропорта (кроме ситуаций, связанных с безопасностью полетов). Д07. Эвакуация ВС с летного поля, если его занятость произошла по вине службы движения. Д11. Временные режимы (включая время официальных церемоний встречи и проводов).
Я	Служба ЭРТОС	Я01. Отказы и неисправности средств радиотехнического обеспечения полетов.
Э	Служба ЭСТОП	Э01. Отказы и неисправности электросветотехнических средствобеспечения полетов. Э02. Отказы и неисправности резервных источников электропитания службы. Э03. Отказы и неисправности внутриаэропортового электроснабжения. Э04. Отказы и неисправности светосигнального обеспечения полетов.
У	ПДСП	У07. Несвоевременное внесение изменений в расписание, если функции работы с расписанием выполняются ПДСП.
Р	Служба режима	Р03. Ограничение приема и выпуска ВС по сигналу "Набат" и др.
Ж	Метеослужба	Ж03. Отказы метеорологического оборудования, установленногона аэродроме для обеспечения посадок ВС по метеоминимумам I, II и III категорий.
М	Метеоусловия	М01. На аэродроме вылета фактическая погода ниже минимума, установленного для взлета.

		M02. Прогноз и фактическая погода в пункте посадки, на запасных аэродромах и по маршруту не позволяет принять решение на вылет в соответствии с требованиями НПП. M06. Сбойная ситуация из-за скоплений ВС в аэропорту по метеоусловиям или занятости воздушного пространства зоны УВД аэродрома по метеоусловиям. M07. Задержки от начала опасного для авиации метеорологического явления до устранения его последствий (уборка снега, гололеда) в сроки, установленные НАС ГА. M10. Запреты полетов, связанные с проведением противоградовых стрельб.
X	Задержки по вине ведомственной авиации и при конфликтных ситуациях	X01. Занятость летного поля по вине ведомственной авиации всвязи со стихийными бедствиями и авариями. X02. Временное закрытие аэропорта из-за конфликтных ситуаций.

Непредвиденные ситуации в аэропортах и отклонения от графика полетов оказывают значительное влияние на различные аспекты аэропортовой деятельности, включая:

- Ограниченное время для принятия оперативных решений;
- Ключевые показатели эффективности (KPI – key performance indicators), отражающие производительность аэропорта;
- Права пассажиров на компенсацию за задержки, регулируемые международными и национальными законами;
- Обеспечение безопасности полетов.

Управление аэропортом в таких условиях требует быстрого и эффективного решения проблем для достижения главной цели — повышения производственной эффективности. В этом ключевую роль играют автоматизированные системы управления, такие как система “КОБРА” с модулем “СПП-ССЭ”, успешно внедренная в 20 аэропортах страны и за ее пределами, что подтверждено актами внедрения. [1]

2. Разработка модели алгоритма корректирующих действий и описание предложенной модели по устранению нарушений регулярности полетов

В данной главе представлена методика, разработанная для руководителей подразделений. Эта методика направлена на совершенствование контроля за состоянием регулярности полётов, проведение постоянного мониторинга, определение причин задержек отправления и вылета, проведение системного анализа регулярности, разработку корректирующих мероприятий с целью предупреждения повторяемости причин задержек отправления и достижение приемлемого уровня состояния регулярности полётов, определенного политикой Главного оператора аэропорта.

Руководитель подразделения, на которое возложена ответственность за произошедшее нарушение регулярности полётов, ответственный за расследование причин задержек отправления и вылета, должен выполнить следующие действия:

- провести анализ полученной информации о произошедшей задержке отправления и вылета воздушного судна и причин к ним приведших;
- в случае несогласия с установленной ПДСА (ПДСА – производственно-диспетчерская служба аэропорта) причиной нарушения регулярности полётов, провести служебное расследование в течении рабочей смены и представить результаты своего расследования в Таблице корректирующих действий по задержкам отправления воздушных судов;
- выработать и провести корректирующие мероприятия, направленные на исключение нарушения регулярности полётов или снижения уровня нарушений до приемлемого состояния и представить мероприятия в Таблице корректирующих действий по задержкам отправления воздушных судов;
- заполненную Таблицу корректирующих действий по задержкам отправления воздушных судов направить в течении рабочей смены в адрес Первого заместителя генерального директора и отдела качества и экономической безопасности.

Таблица 2 – Таблица корректирующих действий по задержкам отправления воздушных судов

Дата выполнения задержанного рейса	Номер рейса /маршрут/ время задержки	Тип ВС /регистрация ВС	Причина задержки отправления воздушного судна, установленная ПДСА	Причина задержки отправления воздушного судна	Корректирующие действия	Срок исполнения
20.08.1980	СУ 7777/Казань - Вашингтон/ 00.03	Ил-96/ RA - 96122	Поздняя регистрация пассажиров из-за сбоя в работе системы регистрации авиаперевозчика	В системе регистрации авиаперевозчика SABRE отсутствовали списки пассажиров	Связались со сменными технологами системы регистрации авиаперевозчика Аэрофлот для оперативного восстановления списков пассажиров	Выполнено

«МЕТОДИКА КОРРЕКТИРУЮЩИХ МЕРОПРИЯТИЙ ПО НАРУШЕНИЯМ РЕГУЛЯРНОСТИ ПОЛЁТОВ ВОЗДУШНЫХ СУДОВ»

1. Настоящая методика разработана для руководителей подразделений в целях совершенствования контроля за состоянием регулярности полётов, проведения постоянного мониторинга, определения причин задержек отправления и вылета, проведения системного анализа регулярности, разработки корректирующих мероприятий с целью предупреждения

повторяемости причин задержек отправления и достижения приемлемого уровня состояния регулярности полётов, определенного политикой Главного оператора аэропорта.

2. Руководитель подразделения, на которое возложена ответственность за произошедшее нарушение регулярности полётов, ответственный за расследование причин задержек отправления и вылета, должен:

- провести анализ полученной информации о произошедшей задержке отправления и вылета воздушного судна и причин к ним приведших;
- в случае несогласия с установленной ПДСА причиной нарушения регулярности полётов, провести служебное расследование в течении рабочей смены и представить результаты своего расследования в Таблице корректирующих действий по задержкам отправления воздушных судов;
- выработать и провести корректирующие мероприятия, направленные на исключение нарушения регулярности полётов или снижения уровня нарушений до приемлемого состояния и представить мероприятия в Таблице корректирующих действий по задержкам отправления воздушных судов;
- заполненную Таблицу корректирующих действий по задержкам отправления воздушных судов направить в течении рабочей смены в адрес Первого заместителя генерального директора и отдела качества и экономической безопасности.

2.1. Ответственность за нарушение регулярности полетов

За нарушение регулярности полетов ВС, независимо от их принадлежности, несут ответственность:

2.1.1. Непосредственный исполнитель - за своевременное и качественное выполнение технологических операций при подготовке ВС к отправлению или при подготовке комплекса наземного обеспечения полетов к работе.

2.1.2. Старший диспетчер (диспетчер) оперативных смен служб предприятия - за оперативное руководство и координацию деятельности всех производственных звеньев по выполнению технологических операций, связанных с обеспечением суточного плана и регулярности полетов, за своевременность и достоверность информации, передаваемой в соответствии с Табелем внутриаэропортовой информации.

2.1.3. Командир ВС - за своевременную подготовку экипажа и выполнение полета в соответствии с полученным заданием.

2.1.4. Руководитель службы (смены) предприятия - за организацию выполнения службой (сменой) технологических операций по подготовке ВС или комплекса наземного обеспечения полетов к работе, диспетчеризацию, пооперационный контроль, передачу информации согласно Табелю внутриаэропортовой информации, принимаемые меры по предотвращению задержек.

2.1.5. Руководитель оперативной смены предприятия - за организацию и координацию работы оперативных смен служб при подготовке ВС к отправлению, подготовку к работе комплекса наземного обеспечения полетов, принятие мер по предотвращению задержек, объективность определения их причин, правильность их оформления и учета, достоверность и своевременность представления отчетности по регулярности полетов ВС в оперативной смене.

2.1.6. Начальник ПДСП (ПДСП - производственно-диспетчерская служба) - за оперативное руководство службами авиапредприятия по обеспечению регулярности полетов, качественную разработку мероприятий по совершенствованию взаимодействия служб при подготовке ВС к отправлению, объективное определение причин задержек, правильность учета и отчетности по регулярности полетов.

2.1.7. Заместитель начальника аэропорта по движению - за своевременное составление и обеспечение согласованного суточного плана полетов, согласование и координацию воздушного движения в интересах регулярности полетов со смежными направлениями, военными и гражданскими секторами зональных центров (ЗЦ) и соседними районными центрами (РЦ).

2.1.8. Представитель Аэрофлота за границей - за своевременное выполнение операций, предусмотренных технологическими графиками подготовки ВС в зарубежных аэропортах, своевременность и достоверность информации, представляемой в соответствии с Табелем сообщений о движении ВС.

2.1.9. Руководитель предприятия (аэропорта) и его заместители - за выполнение настоящего Руководства, состояние и обеспечение регулярности полетов и объективность представляемой отчетности по регулярности отправлений ВС.

2.1.10. Начальник управления ГА и его заместители — за состояние и обеспечение регулярности полетов ВС в авиапредприятиях управления. [6]

2.2. Построение модели алгоритма, объяснение принципов работы алгоритма и его основных этапов

Модель методики корректирующих мероприятий по нарушениям регулярности полётов воздушных судов представлена на Рисунке 1.

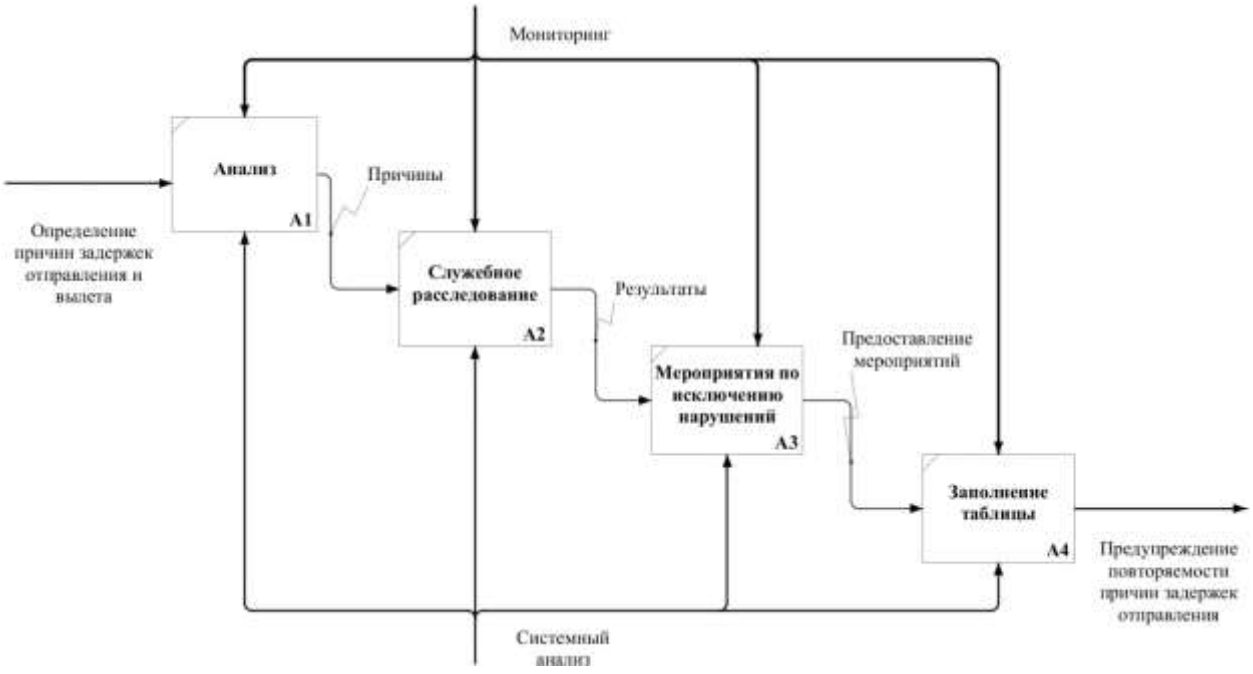

Рисунок 1 – Модель методики корректирующих мероприятий по нарушениям регулярности полётов воздушных судов

Принцип работы этого алгоритма основан на последовательном выполнении следующих шагов:

1. *Анализ информации:* Руководитель подразделения, ответственный за произошедшее нарушение регулярности полётов, проводит анализ полученной информации о задержке отправления и вылета воздушного судна и причин, которые к этому привели.
2. *Служебное расследование*: Если руководитель не согласен с установленной причиной нарушения регулярности полётов, он проводит служебное расследование в течении рабочей смены и представляет результаты своего расследования в Таблице корректирующих действий по задержкам отправления воздушных судов.
3. *Разработка корректирующих мероприятий*: Руководитель вырабатывает и проводит корректирующие мероприятия, направленные на исключение нарушения регулярности полётов или снижения уровня нарушений до приемлемого состояния. Эти мероприятия представляются в Таблице корректирующих действий по задержкам отправления воздушных судов.
4. *Отправка таблицы корректирующих действий:* Заполненная Таблица корректирующих действий по задержкам отправления воздушных судов направляется в течении рабочей смены в адрес Первого заместителя генерального директора и отдела качества и экономической безопасности.

Заключение

Таким образом, этот алгоритм позволяет систематизировать и структурировать процесс управления нарушениями регулярности полётов, что в свою очередь способствует повышению эффективности работы авиакомпании.

Важно отметить, что эффективность алгоритма во многом зависит от качества входных данных, а также от правильности определения причин нарушений и выбора корректирующих мероприятий. Поэтому важно проводить постоянный мониторинг и анализ результатов для обеспечения непрерывного улучшения алгоритма.

Список литературы

1. “Методы ресурсно-временной оптимизации процесса оперативного управления аэропортом в сбойных ситуациях”. 2024. URL: https://www.spbguga.ru/files/2018/Dissovet/Golovchenko/Dissertat_Golovchenko_02.07.2018.pdf (дата обращения: 19.03.2024).
2. “Воздушный кодекс Российской Федерации” ВЗК РФ Статья 40. Аэродромы и аэропорты от 19.03.1997 N 60-ФЗ (ред. от 30.01.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_13744/15bacbc7fb72b52252dff69848c52d3cf2225d95/ (дата обращения: 28.03.2024).
3. “Организация и оптимизация логистических процессов в авиации”. 2024. URL: https://logists.by/blog/organizatsiya-i-optimizatsiya-logisticheskih-protsessov-v-aviatsii-sovremennye-tendentsii-i-unikalnye-resheniya-dlya-effektivnosti-i-bezopasnosti-poletov (дата обращения: 28.03.2024).
4. “Регулярность полетов”. 2024. URL: https://cyberleninka.ru/article/n/k-predotvrascheniyu-sboynyh-situatsiy-v-grazhdanskoy-aviatsii (дата обращения: 19.03.2024).

5. “Сбойные ситуации в авиации”. 2024. URL: https://www.icao.int/Newsroom/Pages/RU/Latest-ICAO-Safety-Report-released.aspx (дата обращения: 19.03.2024).
6. “РРП ГА—90)”. 1990. URL: https://meganorm.ru/Data2/1/4293723/4293723214.pdf (дата обращения: 19.03.2024).

References

1. “Methods of resource-time optimization of the process of operational airport management in emergency situations." 2024. URL: https://www.spbguga.ru/files/2018/Dissovet/Golovchenko/Dissertat_Golovchenko_02.07.2018.pdf (date of application: 03/19/2024).
2. “Air Code of the Russian Federation” of the Russian Federation Air Code Article 40. Airfields and airports dated 03/19/1997 N 60-FZ (as amended on 30.01.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_13744/15bacbc7fb72b52252dff69848c52d3cf2225d95 / (date of access: 03/28/2024).
3. “Organization and optimization of logistics processes in aviation”. 2024. URL: https://logists.by/blog/organizatsiya-i-optimizatsiya-logisticheskih-protsessov-v-aviatsii-sovremennye-tendentsii-i-unikalnye-resheniya-dlya-effektivnosti-i-bezopasnosti-poletov (date of application: 03/28/2024).
4. “Regularity of flights”. 2024. URL: https://cyberleninka.ru/article/n/k-predotvrascheniyu-sboynyh-situatsiy-v-grazhdanskoy-aviatsii (date of application: 03/19/2024).
5. “Aviation failures". 2024. URL: https://www.icao.int/Newsroom/Pages/RU/Latest-ICAO-Safety-Report-released.aspx (date of application: 03/19/2024).
6. “(RRP GA—90)". 1990. URL: https://meganorm.ru/Data2/1/4293723/4293723214.pdf (date of application: 03/19/2024).

Ветров С.Ю. Безопасность микросервисов с помощью SPRING BOOT, SPRING SECURITY и GATEWAY // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 33–39

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

БЕЗОПАСНОСТЬ МИКРОСЕРВИСОВ С ПОМОЩЬЮ SPRING BOOT, SPRING SECURITY И GATEWAY

Ветров С.Ю.
ФГБОУ ВО «МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)», Москва, Россия, (125993, город Москва, Волоколамское ш., д. 4), e-mail: vetrov241201@yandex.ru

Данная статья посвящена анализу и рассмотрению методов обеспечения безопасности в микросервисной архитектуре с использованием инструментов Spring Boot, Spring Security и Spring Cloud Gateway. Мы рассмотрели ключевые аспекты аутентификации и авторизации пользователей, а также роль централизованного шлюза в управлении доступом к микросервисам. Подробно рассмотрены шаги по реализации данного подхода с использованием указанных инструментов и методов обеспечения безопасности передачи данных между клиентом и сервером. В результате статьи читатель получит понимание о том, как создать гибкую и безопасную систему, соответствующую современным требованиям безопасности при разработке микросервисных приложений.

Ключевые слова**:** Микросервисная архитектура, авторизация, аутентификация, API, разработка приложений, backend.

MICROSERVICES SECURITY WITH SPRING BOOT, SPRING SECURITY AND GATEWAY

Vetrov S.Y.
MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: vetrov241201@yandex.ru

This article is devoted to analyzing and reviewing methods of providing security in microservice architecture using Spring Boot, Spring Security and Spring Cloud Gateway tools. We have considered key aspects of user authentication and authorization, as well as the role of a centralized gateway in managing access to microservices. The steps to implement this approach using the specified tools and techniques to secure data transfer between client and server are discussed in detail. As a result of the article, the reader will gain an understanding of how to create a flexible and secure system that meets modern security requirements when developing microservice applications.

Keywords: Microservice architecture, authorization, authentication, API, application development, backend.

Микросервисная архитектура — это некое развитие сервис-ориентированной архитектуры (SOA), направленное на взаимодействие небольших, слабо связанных и легко заменяемых модулей — микросервисов. Микросервис — это изолированная, слабосвязанная единица разработки, работающая над одной задачей [1].

Микросервисная архитектура стала одним из наиболее распространенных подходов к разработке современных приложений. Она позволяет создавать гибкие и масштабируемые системы, разбивая их на небольшие автономные сервисы. Однако при работе с

микросервисами встает вопрос об эффективном и безопасном доступе к самим микросервисам. В этой статье мы рассмотрим использование Spring Boot, Spring Security и Gateway для реализации авторизации посредством сессий в микросервисной архитектуре.

Рассмотрим пример: Проект, реализованный с использованием микросервисной архитектуры. Пользователи могут делиться информацией об интересных событиях и находить компанию для участия в них. Могут отправлять заявки на участие в событиях и оставлять к ним комментарии. Так же есть функционал администратора.

Выделяются 3 микросервиса (рисунок 1):

events – микросервис для работы с событиями;

requests – микросервис для работы с заявками;

comments – микросервис для работы с комментариями.

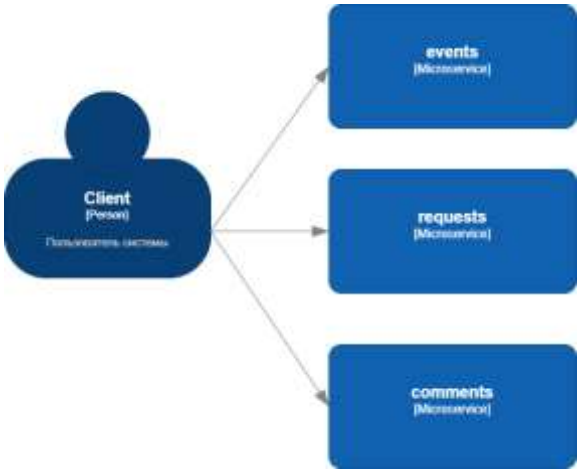

Рисунок 1 – Микросервисы

Как же нам организовать авторизацию пользователя, чтобы понимать какой пользователь обращается к микросервису.

Вариант 1. Отдельный микросервис для авторизации.

Добавляется новый микросервис Auth Service (Рисунок 2), который работает с таблицей users, а другие микросервисы, после получения запросов от пользователя, делают запрос на микросервис авторизации.

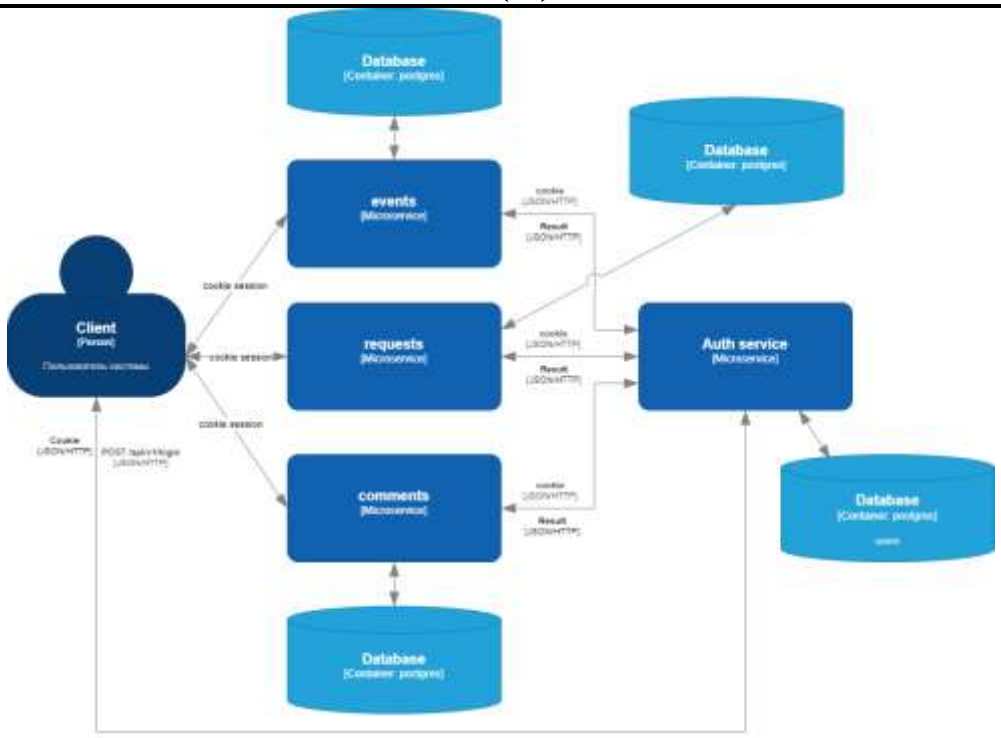

Рисунок 2 – Вариант 1

В данном сценарии, процесс начинается с того, что клиент отправляет запрос на микросервис аутентификации через метод POST (/api/v1/login). Если предоставленные логин и пароль верны, клиент получает в ответ ключ сессии, который сохраняется в куки. Затем клиент использует этот ключ для отправки запроса на целевой микросервис.

После выполнением запроса к целевому микросервису (например, GET /api/v1/events), сам микросервис инициирует запрос к микросервису аутентификации для проверки сессии. Если пользователь успешно аутентифицирован и у него есть доступ к этому ресурсу, то происходит выполнение запроса на выборку событий и передача их клиенту. В случае, если аутентификация не подтверждена, возвращается ошибка с кодом 401 Unauthorized, уведомляя клиента о необходимости повторной аутентификации.

Проблемы этого варианта:

- Каждый микросервис должен выполнять свою роль, а в этом случае, ему необходимо делать дополнительные действия по валидации сессии;
- Микросервисы содержат разные пути, и придётся прописывать логику какие пути требуют авторизацию, а какие нет.

Вариант 2. Использование Api Gateway.

Здесь добавляется новый микросервис Api Gateway, далее шлюз [2]. У шлюза есть конфигурационный файл, в котором прописано, какой путь куда отправлять, например, GET **gateway**/api/v1/events, запрос на получение вообще всех событий. Шлюз должен направить этот запрос на **events**/api/v1/events, то есть на другой микросервис. Вернёмся к нашему случаю (рисунок 3). Шлюз получает запрос от клиента, например на получение всех своих событий. Запрос будет выглядеть так: GET /api/v1/user/events. В самом запросе идентификатор пользователя не указан. В шлюзе сначала идёт запрос на сервис авторизации, там проверяется,

если доступ у этого пользователя и далее подменяется запрос с GET /api/v1/**user/events** на GET /api/v1/**user/1/events**. Что изменилось. Добавился идентификатор пользователя. Сервер авторизации проверил сессию и вернул в шлюз этот идентификатор. И получается, что сам микросервис событий просто вернёт список событий именно этого пользователя, никакой проверки внутри микросервиса нет.

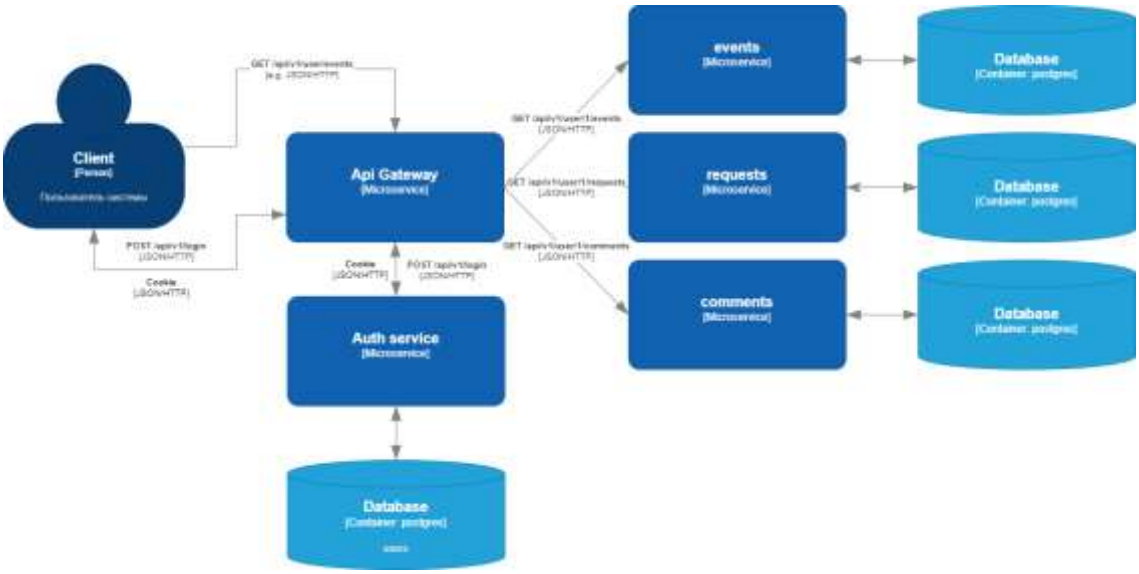

Рисунок 1 – Вариант 2

Проблемы этого варианта:

- Придётся писать конфигурации в шлюзе для каждого пути;
- На каждый запрос приходится ещё 2 дополнительных запроса:

клиент → шлюз → сервис авторизации → целевой микросервис.

Практическая реализация.

Для реализации второго варианта будет использоваться фреймворк Spring Boot 3.2.2, Spring Security 6 и Spring Cloud Gateway 4.1.1.

Сервис авторизации.

Для начала нужно создать проект на сайте start.spring.io и выбрать две зависимости: Spring Web и Spring Security.

Далее создаём конфигурационный класс и в нём создаём бин, в котором определяются настройки авторизации.

Код SecurityConfig

```
    @Bean
public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {
  http
        .csrf(AbstractHttpConfigurer::disable)
        .cors(AbstractHttpConfigurer::disable)
        .headers(h -> h.frameOptions(HeadersConfigurer.FrameOptionsConfig::disable))
        .anonymous(AbstractHttpConfigurer::disable)
        .requestCache(RequestCacheConfigurer::disable)
        .formLogin(form -> form.usernameParameter("usernameOrEmail").loginPage("/login").disable())
```

```
        .httpBasic(AbstractHttpConfigurer::disable)
        .logout(l -> l.logoutUrl("/logout").invalidateHttpSession(true).clearAuthentication(true).disable())
        .securityContext((securityContext) -> securityContext.requireExplicitSave(false))
        .sessionManagement(s -> s.sessionCreationPolicy(SessionCreationPolicy.IF_REQUIRED)
                .maximumSessions(1)
                .maxSessionsPreventsLogin(false)
                .sessionRegistry(sessionRegistry)
        )
        .authorizeHttpRequests((authorize) -> authorize
                .requestMatchers("/users/**").authenticated()
                .requestMatchers("/user/**").authenticated()
                .requestMatchers("/todos/**").authenticated()
                .requestMatchers("/admin/**").hasRole("ADMIN")
                .requestMatchers("/data/user/**").authenticated()
                .requestMatchers("/test").authenticated()
                .requestMatchers("/test2").authenticated()
                .anyRequest().permitAll()
        )
        .addFilterAfter(newLoginFilter, UsernamePasswordAuthenticationFilter.class)
        .exceptionHandling(c -> c.authenticationEntryPoint(new HttpStatusEntryPoint(HttpStatus.UNAUTHORIZED)));
    return http.build();
}
```

Самое главное выделено жирным шрифтом, там определяются пути, которые будут доступны всем, только авторизованным пользователям или пользователям с определёнными ролями. Например, пути /users/** доступны только для авторизованных, а /admin/** только для пользователей с ролью администратора.

Api gateway.

Создаём проект на сайте start.spring.io и выбираем две зависимости: Spring Web и Gateway.

Далее создаём файл конфигурации application.yaml и прописываем правила, по которым будут распределяться маршруты.

Фрагмент файла application.yaml

```
        routes:
    - id: event-route
      uri: http://localhost:7989
      predicates:
        - Path=/user/events/**
      filters:
        - name: AccessSecurityFilter
        - name: AssignUserSecurityFilter
```

Тут назначается идентификатор маршрута, url, на который будет перенаправляться маршрут, и сам путь. Далее идёт фильтры в который как раз и будет подставляться идентификатор пользователя.

В AccessSecurityFilter происходит запрос на сервис авторизации и проверка сессии. Если пользователь прошёл проверку, то фильтр передаёт запрос дальше.

Код AccessSecurityFilter

```
    @Override
public GatewayFilter apply(Config config) {
    return (exchange, chain) -> {
        HttpCookie sessionCookieValue = exchange.getRequest().getCookies().getFirst("SESSION");
        if (sessionCookieValue == null) {
            return Mono.error(new ResponseStatusException(HttpStatus.UNAUTHORIZED, "Unauthorized"));
        } else {
            String requestPath = exchange.getRequest().getPath().toString();
            return webClientBuilder.build()
                    .get()
                    .uri(authServiceUrl + requestPath)
                    .header(HttpHeaders.COOKIE, sessionCookieValue.toString())
                    .exchange()
                    .flatMap(response -> {
                        if (response.statusCode().equals(HttpStatus.NOT_FOUND) ||
response.statusCode().equals(HttpStatus.OK)) {
                            return chain.filter(exchange);
                        } else {
                            return Mono.error(new ResponseStatusException(HttpStatus.UNAUTHORIZED, "Unauthorized)))"));
                        }
                    });
        }
    };
}
```

В AssignUserSecurityFilter происходит подстановка идентификатора пользователя, на красной строке.

Код AssignUserSecurityFilter

```
    @Override
public GatewayFilter apply(Config config) {
    return (exchange, chain) -> {
        HttpCookie sessionCookieValue = exchange.getRequest().getCookies().getFirst("SESSION");
        if (sessionCookieValue == null) {
            return Mono.error(new ResponseStatusException(HttpStatus.UNAUTHORIZED, "Unauthorized"));
        }

        return webClientBuilder.build()
                .get()
                .uri(authServiceUrl + "/user")
                .header(HttpHeaders.COOKIE, sessionCookieValue.toString())
                .retrieve()
                .bodyToMono(UserFullDto.class)
                .flatMap(user -> {
                    ServerHttpRequest request = exchange.getRequest();
                    String originalPath = request.getPath().value();
                    String modifiedPath = originalPath.replace("/user/", "/user/" + user.getId() + "/");
                    ServerHttpRequest modifiedRequest = request.mutate().path(modifiedPath).build();
                    return chain.filter(exchange.mutate().request(modifiedRequest).build());
                })
```

```
            .onErrorResume(error -> Mono.error(new ResponseStatusException(HttpStatus.UNAUTHORIZED,
"Unauthorized")));
    };
}
```

Заключение.

В данной статье мы рассмотрели два варианта организации авторизации пользователей в микросервисной архитектуре.

Первый вариант предполагает создание отдельного микросервиса для авторизации, который обрабатывает запросы от других микросервисов и осуществляет проверку сессий. Этот подход более простой, но требует каждому микросервису выполнять дополнительные действия по валидации сессии.

Второй вариант использует API Gateway для управления доступом к микросервисам. Здесь шлюз направляет запросы на сервис авторизации для проверки доступа пользователя. После успешной аутентификации шлюз подменяет запросы, добавляя идентификатор пользователя. Этот подход позволяет централизованно управлять авторизацией и уменьшает нагрузку на отдельные микросервисы, но требует дополнительных запросов и конфигураций в шлюзе.

В практической реализации второго варианта были использованы фреймворки Spring Boot, Spring Security и Spring Cloud Gateway.

Выбор конкретного варианта зависит от требований к безопасности, гибкости и производительности системы, а также от ее архитектурных особенностей. При правильной реализации оба варианта позволяют создать безопасную и удобную для использования систему, соответствующую современным стандартам разработки микросервисных приложений.

Список литературы

1. Аутентификация и авторизация в проекте с микросервисной архитектурой: стратегии, практический пример. — Текст : электронный//Harb: [сайт]. — URL: https://habr.com/ru/companies/spectr/articles/715290.
2. Pattern: API Gateway / Backends for Frontends. — Текст : электронный//microservices.io : [сайт]. — URL: https://microservices.io/patterns/apigateway.html.
3. Microservices with Spring. — Текст: электронный//Spring: [сайт]. — URL: https://spring.io/blog/2015/07/14/microservices-with-spring.

References

1. Authentication and authorization in a project with a micro-service architecture: strategies, a practical example. — Text : electronic//Harb : [website]. — URL: https://habr.com/ru/companies/spectr/articles/715290.
2. Pattern: API Gateway / Backends for Frontends. — Text : electronic // microservices.io : [website]. — URL: https://microservices.io/patterns/apigateway.html.
3. Microservices with Spring. — Text : electronic//Spring : [website]. — URL: https://spring.io/blog/2015/07/14/microservices-with-spring.

Балуева М.А., Кириллина Ю.В. Автоматизация бизнес-процесса «Продажа кондитерской продукции» на малом производственном предприятии// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 40–45

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.91

АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССА «ПРОДАЖА КОНДИТЕРСКОЙ ПРОДУКЦИИ» НА МАЛОМ ПРОИЗВОДСТВЕННОМ ПРЕДПРИЯТИИ

Балуева М.А., [1]Кириллина Ю.В.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: [1]jvk05@mail.ru

В статье описываются проблемы выполнения бизнес-процесса продажи кондитерской продукции на малом производственном предприятии, для устранения которых предлагается внедрение информационной системы. Для решения вопроса о внедрении информационной системы проведен обзор существующих на рынке программного обеспечения программных продуктов, позволяющих устранить выделенные проблемы, обоснован отказ от их применения. Выбор в пользу собственной разработки дополнен постановкой задачи на разработку информационной системы поддержки продаж.

Ключевые слова: Информационная система, поддержка продаж, автоматизация, функциональные требования, нефункциональные требования, входная информация, выходная информация.

AUTOMATION OF THE BUSINESS PROCESS "SALE OF CONFECTIONERY PRODUCTS" AT A SMALL MANUFACTURING ENTERPRISE

Balueva M.A., [1]Kirillina Yu.V.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: [1]jvk05@mail.ru

The article describes the problems of performing the business process of selling confectionery products in a small manufacturing enterprise, to eliminate which the introduction of an information system is proposed. To solve the issue of the introduction of an information system, a review of existing software products on the software market was conducted to eliminate the identified problems, and the refusal to use them was justified. The choice in favor of in-house development is complemented by the task of developing an information sales support system.

Keywords: Information system, sales support, automation, functional requirements, non-functional requirements, input information, output information.

В современном мире растущая конкуренция в бизнесе делает эффективное управление бизнес-процессами важным звеном успеха для предприятий. Использование информационных технологий позволяет не только оптимизировать процессы, но и повысить успешность ведения бизнеса в целом [1].

Основным методом автоматизации бизнес-процессов организации можно считать внедрение информационной системы, это способствует улучшению мониторинга процесса и управления ими [1].

На основе проведенного исследования одного из малых производственных предприятий, специализирующегося на изготовлении и реализации кондитерской продукции, в качестве основных проблем бизнес-процесса продажи кондитерской продукции было выделено:

1. Задействование в данном процессе большого количества сотрудников внешних структурных подразделений относительно отдела, в котором протекает бизнес-процесс.

2. Использование пакета программного обеспечения Microsoft Office для оформления документов, сопровождающих выполнение процесса. В таком случае возникает потребность ручного ввода необходимой информации, что является неоправданными временными затратами. Кроме того, ручное внесение и вычисление показателей для отчетности несет за собой высокую вероятность неточностей [2].

Вследствие этого автоматизация процесса продажи на предприятии не только позволит регламентировать внутренние операции организации, но и будет способствовать укреплению ее конкурентоспособности и повышению удовлетворенности клиентов.

На рынке программных продуктов присутствуют готовые информационные системы, которые могут устранить описанные проблемы бизнес-процесса. Для сравнения существующих разработок в данной области выбраны программные продукты «Битрикс24», ERP-сервис «МойСклад», «Мегаплан» [3, 4, 5].

Требуемое оборудование под каждый программный продукт представлено ниже:

1. «Битрикс24»: персональный компьютер, мобильное устройство, сервер предприятия.

2. ERP-сервис «МойСклад»: персональный компьютер, мобильное устройство.

3. «Мегаплан»: персональный компьютер, мобильное устройство, сервер предприятия.

Главная проблема существующих разработок — низкая адаптация под бизнес, занимающийся изготовлением и продажей пищевой продукции, высокая перегруженность систем сложным функционалом, долгое обучение персонала работе в системе, сложная интеграция уже существующих процессов, а также вероятно, возникнет необходимость перестроения устоявшихся процессов с учетом возможностей системы [1]. При этом в рассмотренных системах отсутствует полный набор документов, используемых в бизнес-процессе (Таблица 1).

Таблица 1 – Обзор существующих разработок

Программный продукт	**Функционал**	**Стоимость (руб.)**	**Характеристики**
«Битрикс24»	Ведение клиентской базы; ведение истории сделок; автоматизация продаж; поддержка любых видов оплаты; формирование документов; оформление доставки; отчеты	От 1990 руб. в мес. за 5 пользователей за облачную версию и 109 000 руб. в год за коробочную версию. Есть пробная версия	Подходит для крупного и среднего бизнеса, поддерживает любые типы операционных систем
«МойСклад»	Работа с клиентами; поддержка первичных документов; мониторинг и анализ показателей деятельности	6714 руб. в год на 10 сотрудников за облачную версию	Подходит для малого и среднего бизнеса, поддерживает любые типы операционных систем
«Мегаплан»	Единая клиентская база; контроль менеджеров; история взаимодействий с клиентом; воронка продаж; отчетность; шаблоны документов; финансовый учет	От 559 руб. в мес. за 1 пользователя за облачную версию и от 75 000 руб за 10 сотрудников за коробочную версию. Есть пробная версия	Подходит для малого и среднего бизнеса, поддерживает любые типы операционных систем

Целесообразным решением для небольшого предприятия будет разработка собственной информационной системы поддержки продаж, которая ориентирована на производимую продукцию и существующую структуру процессов отдела сбыта. Система также должна быть специализирована для поддержки продажи пищевой продукции юридическим лицам, что накладывает определенные требования к входной, выходной и хранимой информации.

Для внедрения информационной системы в деятельность предприятия, необходимо определить ее тип, выделив основной функционал будущей системы [1].

Информационная система поддержки продаж должна отвечать следующим функциональным требованиям:

- внесение, хранение, поиск данных о заказах покупателей;
- внесение, хранение, поиск данных о покупателях и их представителях;
- внесение, хранение, поиск данных о сотрудниках организации;
- внесение, хранение, поиск данных о кондитерской продукции;
- выгрузка, загрузка сертификатов соответствия продукции;
- внесение, хранение, поиск данных об оплатах;
- выгрузка, загрузка, хранение, поиск документов: договор купли-продажи, счет на оплату, счет-фактура, накладная на отпуск материалов на сторону, товарная накладная;
- формирование отчетности по заданным критериям.

Входной информацией для системы будет заявка покупателя, менеджер по сбыту будет обрабатывать несколько заявок за один рабочий день. Также к входной информации относятся:

- перечень сотрудников отдела сбыта;
- перечень кондитерской продукции, производимой организацией;
- сертификат соответствия продукции, дополняющий договор купли-продажи;
- кассовый чек, являющийся подтверждением наличной оплаты.
- Выходной информацией будет:
- договор купли-продажи;
- счет на оплату;
- счет-фактура;
- накладная на отпуск материалов на сторону [2];
- товарная накладная.

Первые два документа будут формироваться для каждой заявки клиента, остальные только для оплаченных заявок.

Также выходной информацией будет выступать:

- отчет об остатках продукции на складах;
- отчет о выполнении заказов;
- отчет о прибыли от продажи вида продукции;
- отчет о производительности процесса продажи;
- отчет о рентабельности вида продукции;
- отчет по клиентам.

Данные отчеты будут формироваться отделом сбыта каждый месяц.

Пользователями системы будут руководитель отдела сбыта и менеджер по сбыту.

Менеджер по сбыту будет использовать информационную систему для создания и обработки заказов клиентов. Ему будет доступно внесение данных продукции, покупателей и их представителей, данных заказов и их оплат, формирование, загрузка и выгрузка необходимой документации, формирование и выгрузка отчетности.

Руководитель отдела сбыта будет использовать информационную систему для мониторинга производительности сотрудников отдела, анализа данных о заказах, клиентах, продажах, продукции (с помощью формирования и выгрузки отчетности), выгрузки и загрузки документов по заказам.

На Рисунке 1 представлена диаграмма вариантов использования. На ней отражены роли, необходимые в информационной системе, и соответствующий им функционал.

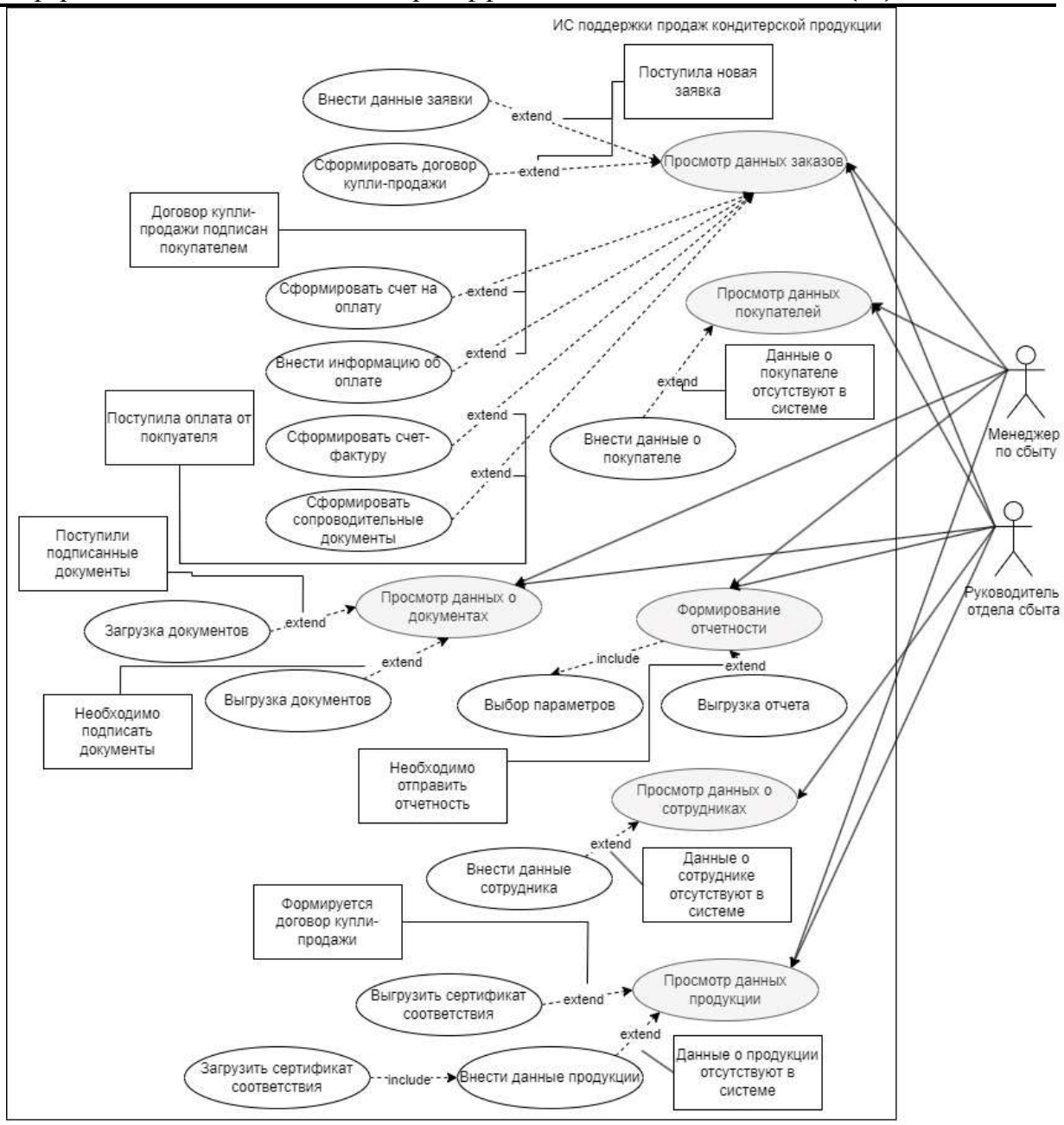

Рисунок 1 – Диаграмма вариантов использования

К нефункциональным требованиям информационной системы поддержки продаж кондитерской продукции стоит отнести:

- организация хранения документов в облачном хранилище;
- работа с системой в браузере;
- производительность системы: время отклика не должно превышать 1 минуты;
- защита данных сотрудников и клиентов: система должна быть защищена от несанкционированного доступа;
- масштабируемость: система должна поддерживать добавление нового функционала и пользователей;
- доступность системы в любое время;
- поддержка русского языка.

Таким образом, в результате анализа проблем, связанных с бизнес-процессом продажи кондитерской продукции на малом производственном предприятии, а также обзора существующих программных продуктов для устранения проблем, сделан вывод о необходимости разработки собственной информационной системы поддержки продаж, которая будет ориентирована на потребности предприятия и позволит:

- собрать воедино информационные потоки бизнес-процесса;
- свести необходимость ручного ввода информации к минимуму;
- исключить участие сотрудников отделов, являющихся внешними структурными подразделениями для отдела сбыта;
- сократить временные затраты на выполнение бизнес-процесса;

что положительно скажется на повышении эффективности работы отдела сбыта малого производственного предприятия.

Список литературы

1. Харитонов, Ю. В., Нелюбина, Ю. А. Моделирование бизнес-процессов торгового предприятия с целью внедрения автоматизированной информационной системы // Новое в экономической кибернетике — 2020. —№ 1. — С. 78-90. — URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://elibrary.ru/download/elibrary_44098822_53042733.pdf (дата обращения 25.03.2024).
2. Печенкина, М. Е. Электронный документооборот операций по продаже готовой продукции // Государство и право: проблемы и перспективы совершенствования : сборник научных трудов 5-й Международной научной конференции — Курск. — 2022. —С.202-206.—URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https: //www.elibrary.ru/download/elibrary_49564157_12809426.pdf(дата обращения 25.03.2024).
3. МойСклад: [сайт]. URL: https://www.moysklad.ru/ (дата обращения 25.03.2024)
4. Битрикс24 : [сайт]. URL: https://www.bitrix24.ru/ (дата обращения 25.03.2024)
5. Мегаплан : [сайт]. URL: https://megaplan.ru/ (дата обращения 25.03.2024)

References

1. Kharitonov, Yu. V., Nelubina, Yu. A. Modeling of business processes of a trading enterprise with a purpose of introducing an automated information system // New in economic cybernetics — 2020. — No. 1. — pp. 78-90. — URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://elibrary.ru/download/elibrary_44098822_53042733.pdf (accessed 25.03.2024).
2. Pechenkina, M. E. Electronic document management of operations for the sale of finished products // State and law : problems and prospects for improvement : collection of scientific papers of the 5th International Scientific Conference —Kursk. — 2022. — pp. 202-206. — URL: chrome—extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.elibrary.ru/download/elibrary_49564157_12809426.pdf (accessed 25.03.2024).
3. MyAccount : [website]. URL: https://www.moysklad.ru/ (accessed 25.03.2024)
4. Bitrix24 : [website]. URL: https://www.bitrix24.ru/ (accessed 25.03.2024)
5. Megaplan : [website]. URL: https://megaplan.ru/ (accessed 25.03.2024)

Удальцов К.Р. Влияние интернета вещей на кибербезопасность: уязвимости подключенных устройств// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 46–49

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ВЛИЯНИЕ ИНТЕРНЕТА ВЕЩЕЙ НА КИБЕРБЕЗОПАСНОСТЬ: УЯЗВИМОСТИ ПОДКЛЮЧЕННЫХ УСТРОЙСТВ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья исследует влияние Интернета вещей (IoT) на кибербезопасность и предлагает ряд стратегий для улучшения безопасности IoT. Рассматриваются ключевые аспекты, такие как образование пользователей и производителей, развитие технологий киберзащиты, международное сотрудничество и стандартизация. Настоятельная необходимость совместных усилий пользователей, производителей, правительств и международного сообщества для обеспечения безопасного развития Интернета вещей подчеркивается как ключевой момент в минимизации уязвимостей IoT к киберугрозам.

Ключевые слова: Интернет вещей, кибербезопасность, IoT устройства, обучение пользователей, производители IoT, технологии киберзащиты, международное сотрудничество, стандартизация, киберугрозы, уязвимости IoT.

THE IMPACT OF THE INTERNET OF THINGS ON CYBERSECURITY: VULNERABILITIES OF CONNECTED DEVICES

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article explores the impact of the Internet of Things (IoT) on cybersecurity and suggests a number of strategies to improve IoT security. Key aspects such as the education of users and manufacturers, the development of cyber defense technologies, international cooperation and standardization are considered. The urgent need for joint efforts by users, manufacturers, governments and the international community to ensure the safe development of the Internet of Things is highlighted as a key point in minimizing IoT vulnerabilities to cyber threats.

Keywords: Internet of Things, cybersecurity, iOS devices, user training, It manufacturers, cyber defense technologies, international cooperation, standardization, cyber threats, IoT vulnerabilities.

Интернет вещей (IoT) - это концепция, которая описывает сеть подключенных устройств, способных обмениваться данными между собой без прямого участия человека. Эти устройства могут включать все, начиная от умных домашних приборов и кончая медицинскими устройствами и промышленным оборудованием. Однако с развитием IoT возникают новые вызовы в области кибербезопасности.[1]

1. Увеличение атак на подключенные устройства

В силу того, что большое количество устройств в IoT работает на основе встраиваемых систем и операционных систем, они могут быть более уязвимы к кибератакам. Атаки могут включать в себя взлом устройств, перехват данных или даже использование устройства для организации DDoS-атак на другие системы.

2. Недостатки в конструкции и защите

Многие устройства IoT разрабатываются с упором на функциональность и экономию ресурсов, что может привести к недостаточной защите от киберугроз. [2] Некоторые устройства могут иметь стандартные пароли, слабую или отсутствующую защиту данных, что делает их легкими целями для злоумышленников.

3. Оценка рисков и совершенствование мер безопасности

Для смягчения рисков, связанных с IoT, необходимо провести оценку уязвимостей и реализовать более строгие стандарты безопасности. [3] Меры также могут включать в себя широкое использование шифрования данных, улучшение аутентификации устройств и обновление программного обеспечения для устранения обнаруженных уязвимостей.

4. Обзор законодательства и регулирования

Большинство стран начали разрабатывать законодательство, которое регулирует безопасность устройств IoT. [4] Это включает требования к обязательному внедрению стандартов безопасности, отчетности о нарушениях безопасности и наложении штрафов за недостатки в защите.

Интернет вещей, несомненно, привносит огромные выгоды в современную жизнь, однако необходимо активно бороться с уязвимостями безопасности, чтобы предотвратить серьезные угрозы для частных лиц, организаций и общественной инфраструктуры. [5],Путем улучшения стандартов защиты и юридического регулирования мы можем снизить риски и продолжить развитие IoT в безопасном и устойчивом направлении. Обучение пользователей и производителей [6]

Одним из ключевых аспектов улучшения кибербезопасности IoT является образование и обучение пользователям и производителям. Пользователям необходимо осознавать основы безопасного использования устройств IoT, такие как регулярное обновление программного обеспечения, использование надежных паролей и защита своих домашних сетей. Производители же должны уделять большее внимание интеграции безопасности на ранних этапах разработки устройств.[7]

5. Развитие технологий киберзащиты

С постоянным развитием угроз кибербезопасности IoT необходимо активное совершенствование технологий защиты. [8] Это включает в себя использование искусственного интеллекта и машинного обучения для обнаружения и предотвращения атак, разработку средств мониторинга и обнаружения угроз, а также усовершенствование методов шифрования и аутентификации.

6. Международное сотрудничество и стандартизация

Киберугрозы не ограничиваются границами стран, поэтому международное сотрудничество играет ключевую роль в обеспечении безопасности IoT. Важно развивать международные стандарты безопасности, обмениваться информацией о киберугрозах и совместно реагировать на кибератаки.

Заключение

Все большее количество устройств IoT поглощает нашу повседневную жизнь, делая ее более удобной и эффективной. Однако без должной защиты эти устройства могут стать мишенями для киберпреступников, угрожая нашей конфиденциальности, безопасности и даже физическому благополучию. Совместные усилия пользователей, производителей, правительств и международного сообщества необходимы для обеспечения безопасного развития Интернета вещей и минимизации его уязвимостей к киберугрозам.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.

3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.
8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Нижлукченко И.Д. Безопасность мобильных устройств: лучшие практики и приложения. советы по защите личных данных и повышению безопасности смартфонов и планшетов // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 50–55

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ: ЛУЧШИЕ ПРАКТИКИ И ПРИЛОЖЕНИЯ. СОВЕТЫ ПО ЗАЩИТЕ ЛИЧНЫХ ДАННЫХ И ПОВЫШЕНИЮ БЕЗОПАСНОСТИ СМАРТФОНОВ И ПЛАНШЕТОВ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В статье "Безопасность мобильных устройств: лучшие практики и приложения" рассматриваются ключевые аспекты обеспечения безопасности смартфонов и планшетов, которые стали неотъемлемой частью нашей повседневной жизни. С учетом того, что мобильные устройства хранят огромное количество личной информации и обеспечивают доступ к различным онлайн-сервисам, их защита от киберугроз и несанкционированного доступа приобретает особую актуальность. В статье подчеркивается важность комплексного подхода к безопасности, который включает в себя использование надежных паролей, активацию двухфакторной аутентификации, регулярное обновление программного обеспечения и осторожный выбор приложений.

Ключевые слова: Безопасность мобильных устройств, кибербезопасность, защита личных данных, антивирусные приложения, VPN-сервисы, менеджеры паролей, двухфакторная аутентификация, обновление программного обеспечения, безопасное использование приложений, обучение пользователей, цифровая безопасность.

MOBILE DEVICE SECURITY: BEST PRACTICES AND APPLICATIONS. TIPS FOR PROTECTING PERSONAL DATA AND IMPROVING THE SECURITY OF SMARTPHONES AND TABLETS

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

The article "Mobile Device Security: Best Practices and Applications" examines the key aspects of smartphone and tablet security that have become an integral part of our daily lives. Given that mobile devices store a huge amount of personal information and provide access to various online services, their protection from cyber threats and unauthorized access is becoming particularly relevant. The article highlights the importance of a comprehensive approach to security, which includes the use of strong passwords, activation of two-factor authentication, regular software updates and careful application selection.

Keywords: Mobile device security, cybersecurity, personal data protection, antivirus applications, VPN services, password managers, two-factor authentication, software updates, safe use of applications, user training, digital security.

В эпоху цифровизации безопасность мобильных устройств выходит на первый план. Смартфоны и планшеты служат порталом в мир широких цифровых возможностей, однако также они представляют собой уязвимую точку, через которую могут быть реализованы атаки на вашу приватность и безопасность данных. Утечки данных, фишинг, вредоносные программы — лишь вершина айсберга потенциальных угроз.

В современном мире, где границы между цифровым и физическим пространствами стираются, мобильные устройства стали неотъемлемой частью нашей жизни. Они хранят в себе ключи к нашей личной и профессиональной жизни, содержат финансовую информацию, личные данные, доступ к социальным сетям и профессиональным инструментам. Именно поэтому вопросы безопасности мобильных устройств приобретают критическую важность. В эру, когда информационные утечки могут привести к серьезным финансовым потерям и ущербу репутации, а кибератаки становятся все более изощренными, защита мобильных устройств не просто вопрос технической безопасности; это вопрос сохранения личной автономии и доверия в цифровом обществе.[4]

Мобильные устройства, будучи постоянно подключенными к интернету, представляют собой идеальную цель для киберпреступников. Они ищут уязвимости не только в операционных системах и приложениях, но и в поведении пользователей, которые часто недооценивают уровень угрозы. Фишинг, вредоносное программное обеспечение, подбор паролей — лишь некоторые из инструментов, используемых злоумышленниками для получения несанкционированного доступа к данным. Учитывая это, безопасность мобильных устройств выходит за рамки простой защиты личной информации; это основа для защиты цифровой идентичности, финансового благополучия и личной безопасности в широком смысле этого слова.

Таким образом, значимость безопасности мобильных устройств в современном мире невозможно переоценить. Она является фундаментом, на котором строятся доверие и безопасность в цифровую эпоху, позволяя пользователям не только защитить свою личную информацию, но и обеспечить уверенность в использовании цифровых технологий для расширения своих возможностей в повседневной жизни и профессиональной деятельности.

Основой защиты данных на мобильных устройствах является комплексный подход, включающий в себя использование надежных паролей и методов биометрической идентификации, активацию двухфакторной аутентификации, а также регулярное обновление операционной системы и приложений.[3] Эти меры могут значительно снизить риск несанкционированного доступа к вашему устройству и данных.

Разработка стратегии безопасности для мобильных устройств представляет собой многоуровневый процесс, который начинается с понимания того, что смартфоны и планшеты являются не просто инструментами для связи или развлечения, а мощными устройствами, хранящими огромное количество личной и чувствительной информации.[1] Этот процесс требует тщательного анализа потенциальных угроз и рисков, с которыми пользователи могут столкнуться, и разработки комплексных мер для их предотвращения или минимизации.

Основой любой стратегии безопасности является создание надежного барьера между личными данными пользователя и потенциальными угрозами. Это достигается путем внедрения сильных паролей и механизмов биометрической идентификации, которые служат первой линией защиты от несанкционированного доступа. Дополнительным слоем защиты

выступает активация двухфакторной аутентификации, предоставляющей еще один уровень проверки подлинности, что значительно усложняет задачу для злоумышленников, желающих получить доступ к устройству или онлайн-аккаунтам пользователя.

Однако технические меры безопасности не ограничиваются только контролем доступа. Важным аспектом является регулярное обновление операционной системы и установленных приложений, которое позволяет не только расширить функционал устройства, но и своевременно устранять обнаруженные уязвимости, тем самым предотвращая возможные атаки.

Комплексный подход к разработке стратегии безопасности также подразумевает осознанное отношение к установке и использованию мобильных приложений. Пользователям рекомендуется скачивать приложения только из проверенных источников, таких как официальные магазины приложений, и внимательно относиться к предоставляемым приложениям разрешениям, избегая тех, которые требуют доступ к чувствительной информации без явной необходимости.

В целом, разработка стратегии безопасности для мобильных устройств является динамичным процессом, требующим регулярного пересмотра и адаптации к постоянно меняющемуся ландшафту угроз. Это не только техническая задача, но и вопрос повышения осведомленности и ответственности пользователей в вопросах цифровой безопасности.

В мире, где каждое мобильное устройство содержит в себе бесчисленное множество приложений, от игр и социальных сетей до финансовых инструментов и рабочих утилит, важность выбора надежных приложений не может быть переоценена.[2] Опасности, связанные с установкой и использованием ненадежных приложений, варьируются от незначительных до катастрофических, включая потерю личной и финансовой информации, ущерб для устройства и даже несанкционированный доступ к личным данным. Поэтому процесс выбора приложений должен быть основан на строгих критериях безопасности и доверия.

Ключевым моментом в выборе безопасных приложений является предпочтение тех, что размещены в официальных магазинах приложений, таких как Google Play Store или Apple App Store. Эти платформы проводят предварительную проверку всех размещаемых на них приложений на предмет соответствия определенным стандартам безопасности и надежности. Однако, даже в этих условиях, важно проводить собственную проверку. Внимательное изучение описаний приложений, отзывов пользователей и рейтингов может предоставить дополнительную информацию о надежности и функциональности приложения.

Критически важным аспектом выбора приложений является анализ требуемых ими разрешений. Многие приложения запрашивают доступ к личной информации или функциям устройства, который не всегда необходим для их работы.[5] В этом контексте, осознанный выбор, при котором пользователь предоставляет доступ только тем приложениям, в которых уверен, и только к той информации, которая необходима для функционирования приложения, становится не просто вопросом удобства, но и защиты.

Таким образом, выбор надежных приложений является сложной задачей, требующей внимательного рассмотрения ряда факторов. От выбора источника загрузки до анализа требуемых разрешений, этот процесс играет ключевую роль в обеспечении безопасности и

конфиденциальности пользователей в цифровом мире. В эпоху, когда мобильные устройства становятся все более интегрированными в нашу повседневную жизнь, осознанный выбор приложений становится неотъемлемой частью защиты нашей цифровой личности.

На рынке существует множество приложений, предназначенных для улучшения безопасности мобильных устройств. Среди них — антивирусы, приложения для управления паролями, VPN-сервисы и приложения для шифрования данных. Использование таких приложений может стать дополнительным слоем защиты в борьбе с угрозами безопасности.

В цифровую эпоху, когда технологии развиваются с невероятной скоростью, безопасность мобильных устройств становится вопросом, требующим особого внимания. Использование специализированных приложений для обеспечения безопасности мобильных устройств является одной из ключевых стратегий защиты личной информации от внешних угроз. Эти приложения разработаны с целью предотвратить несанкционированный доступ, обеспечить конфиденциальность данных и защитить устройства от вредоносного программного обеспечения. Вместо того чтобы рассматривать каждое приложение в отдельности, целесообразнее взглянуть на их использование как на многоуровневую систему защиты, где каждый элемент играет свою роль в общей стратегии безопасности.

Приложения для управления паролями, например, обеспечивают безопасное хранение и генерацию сложных паролей, что существенно снижает риск их подбора или утечки. В то время как VPN-сервисы шифруют интернет-трафик, скрывая ваше местоположение и защищая данные от посторонних глаз, особенно важно это при использовании открытых Wi-Fi сетей. Антивирусные приложения сканируют устройство на наличие вредоносного ПО и предотвращают его установку, тем самым защищая устройство от атак. Приложения для шифрования данных обеспечивают дополнительный уровень защиты, позволяя кодировать личную информацию таким образом, что даже в случае утечки она останется недоступной для неавторизованных лиц.

Таким образом, эффективное использование специализированных приложений для безопасности не просто минимизирует риски, связанные с потерей данных или кибератаками, но и в значительной степени повышает уровень личной безопасности пользователя в цифровом пространстве. Это позволяет пользователям чувствовать себя более уверенно, зная, что их личные данные защищены с помощью современных технологических решений. Важно понимать, что ни одно приложение не может обеспечить абсолютную безопасность, но комплексный подход, включающий использование различных типов специализированных приложений, является ключом к созданию надежной системы защиты мобильных устройств.

Повышение осведомленности пользователей о рисках и методах защиты является неотъемлемой частью стратегии безопасности. Регулярное проведение информационных кампаний, обучающих пользователей основам безопасного поведения в сети, может существенно снизить риск успешных атак на мобильные устройства.

В контексте обеспечения безопасности мобильных устройств обучение пользователей играет столь же важную роль, как и технические средства защиты. Ведь многие угрозы безопасности возникают не из-за недостатков в программном обеспечении, а из-за действий самих пользователей, которые могут неосознанно подвергать себя риску. В этой связи, осведомленность пользователей о потенциальных угрозах и методах их предотвращения становится ключевым элементом комплексной стратегии безопасности.

Основная задача обучения заключается в повышении уровня осведомленности пользователей о различных аспектах безопасности, начиная от основных принципов создания надежных паролей и заканчивая распознаванием фишинговых атак и защитой от вредоносного программного обеспечения. Это включает в себя не только предоставление знаний о том, какие угрозы существуют, но и развитие навыков безопасного поведения в сети, таких как осторожное использование публичных Wi-Fi сетей, проверка подлинности веб-сайтов и приложений, а также осознанный выбор информации, которой пользователь делится онлайн.

Помимо индивидуального обучения, важным аспектом является создание культуры безопасности в организациях, где каждый сотрудник осознает свою роль в защите корпоративных данных. Это может включать регулярные тренинги, симуляции атак, а также информационные кампании, направленные на поддержание высокого уровня осведомленности о вопросах безопасности.

Таким образом, обучение пользователей не просто дополняет технические меры безопасности, но и активно способствует формированию более безопасной цифровой среды. Развивая понимание и умения пользователей в области кибербезопасности, можно значительно снизить риск успешных атак и защитить как личные, так и корпоративные данные от возможных угроз. В конечном итоге, каждый пользователь, осведомленный о рисках и способах их предотвращения, становится важной частью общей системы защиты информации.

В заключение, важно подчеркнуть, что безопасность мобильных устройств в современном мире является многоаспектной задачей, требующей внимательного подхода как со стороны пользователей, так и разработчиков, производителей оборудования и организаций, занимающихся вопросами кибербезопасности. Сочетание технических средств защиты, таких как использование надежных приложений, регулярные обновления программного обеспечения и специализированные инструменты безопасности, с образовательными инициативами, направленными на повышение осведомленности пользователей, создает сильную основу для обеспечения защиты данных и личной информации.

Однако следует признать, что в мире постоянно развивающихся технологий и угроз невозможно достичь абсолютной безопасности. Каждое новое решение в области защиты данных может стать вызовом для злоумышленников, стремящихся найти новые способы обхода систем безопасности. Это означает, что процесс обеспечения безопасности мобильных устройств не является разовой задачей, а требует постоянного внимания, обновления знаний и адаптации к новым условиям.

В этом контексте ключевым аспектом является сотрудничество и обмен знаниями между всеми участниками процесса: пользователями, разработчиками, компаниями, предоставляющими безопасность, и государственными органами. Только совместными усилиями можно достигнуть значительного прогресса в защите цифровой среды и обеспечить безопасность мобильных устройств в долгосрочной перспективе.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Удальцов К.Р. Значение конечного шифрования для защиты конфиденциальности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 56–59

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЗНАЧЕНИЕ КОНЕЧНОГО ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья обсуждает важность конечного шифрования (End-to-End Encryption, E2EE) в контексте защиты конфиденциальности данных. Автор рассматривает преимущества этого метода шифрования, его роль в обеспечении частной жизни, а также значение в сфере бизнеса. Также освещаются вызовы, с которыми сталкивается конечное шифрование, и перспективы его развития в будущем. Статья предназначена для широкой аудитории, включая индивидуальных пользователей, компании и специалистов в области кибербезопасности, а также всех, кто интересуется защитой данных в цифровой эпохе.

Ключевые слова: Конечное шифрование, защита данных, конфиденциальность, кибербезопасность, E2EE, цифровая безопасность, шифрование, приватность, бизнес-сфера, обмен сообщениями, информационная безопасность.

THE VALUE OF END-TO-END ENCRYPTION TO PROTECT DATA PRIVACY

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance of End-to-End Encryption (E2EE) in the context of data privacy protection. The author examines the advantages of this encryption method, its role in ensuring privacy, as well as its importance in the business sphere. It also highlights the challenges faced by end-to-end encryption and the prospects for its development in the future. The article is intended for a wide audience, including individual users, companies and cybersecurity professionals, as well as anyone interested in data protection in the digital age.

Keywords: end encryption, data protection, privacy, cybersecurity, E2EE, digital security, encryption, privacy, business sphere, messaging, information security.

Введение

В современном мире, где информация стала ключевым ресурсом, защита данных и обеспечение их конфиденциальности стали важнейшими задачами. Одним из наиболее надежных методов защиты конфиденциальности данных является конечное шифрование. Этот метод шифрования играет критическую роль в предотвращении несанкционированного доступа к чувствительной информации.

1. Что такое конечное шифрование?

Конечное шифрование (End-to-End Encryption, E2EE) [1] - это способ шифрования данных, который позволяет отправителю и получателю обмениваться информацией, которая остается зашифрованной на всех этапах передачи, а расшифровать её может только предполагаемый получатель. Даже поставщик услуги обмена сообщениями или хранения данных не имеет возможности прочитать содержимое сообщений.

2. Защита от несанкционированного доступа

Одним из ключевых преимуществ конечного шифрования является его способность предотвращать несанкционированный доступ к данным. [1] Благодаря этому методу шифрования, данные остаются защищенными на всех этапах передачи и хранения, что делает практически невозможным их расшифровку третьими лицами без соответствующих ключей.[2]

3. Защита конфиденциальности в цифровых коммуникациях

В сфере цифровых коммуникаций конечное шифрование становится все более важным. [2] При обмене сообщениями через различные платформы, где конфиденциальность имеет первостепенное значение, использование конечного шифрования обеспечивает надежную защиту от перехвата сообщений третьими лицами.

4. Преимущества конечного шифрования [3]

Конечное шифрование обладает неоспоримыми преимуществами, особенно в контексте сохранения конфиденциальности данных. [4] Одним из ключевых аспектов является то, что даже сам провайдер услуги обмена сообщениями или хранения данных не имеет доступа к содержимому сообщений, поскольку оно остается зашифрованным на всех этапах передачи. Это создает непреодолимый барьер для злоумышленников, предотвращая утечку конфиденциальной информации.

5. Значение в сфере бизнеса

В бизнес-среде конечное шифрование становится важным инструментом для защиты коммерческих тайн, финансовой информации и персональных данных клиентов. [3] Благодаря этому методу шифрования компании могут обмениваться конфиденциальной информацией, будучи уверенными в её безопасности, что способствует поддержанию доверия клиентов и партнёров.[5]

6. Вызовы и перспективы

Несмотря на все преимущества, конечное шифрование также сталкивается с вызовами, связанными с законодательством о праве на доступ к данным в различных странах. [4] Некоторые государства стремятся вводить ограничения на использование конечного шифрования из соображений национальной безопасности, что создает сложности для компаний и пользователей, желающих обеспечить конфиденциальность своих данных.

7. Роль конечного шифрования в обеспечении частной жизни [6]

В повседневной жизни конечное шифрование играет важную роль в защите личной информации. Отправляя личные сообщения, фотографии или документы через мессенджеры или электронную почту, люди ожидают, что их данные будут надежно защищены от посторонних глаз. Конечное шифрование обеспечивает эту защиту, создавая прочный барьер для потенциальных нарушителей безопасности.

8. Обзор существующих технологий

На сегодняшний день существует множество технологий, предоставляющих конечное шифрование для различных целей. [7] Мессенджеры, приложения электронной почты, облачные хранилища и другие платформы используют различные методы шифрования для обеспечения безопасности данных своих пользователей. Это свидетельствует о том, что конечное шифрование становится все более распространенным и доступным для широкой аудитории.

9. Будущее конечного шифрования

В будущем конечное шифрование будет продолжать развиваться, стремясь к усовершенствованию методов шифрования и расширению его применения. [8] С постоянным ростом объема цифровых данных и увеличением угроз кибербезопасности, необходимость в надежных методах защиты данных будет только усиливаться, делая конечное шифрование ключевым элементом цифровой безопасности.

Заключение

Конечное шифрование играет важную роль в обеспечении конфиденциальности данных как на уровне индивидуальных пользователей, так и на уровне компаний. Этот метод шифрования обеспечивает защиту от несанкционированного доступа к данным, способствует сохранению доверия пользователей к цифровым сервисам и является неотъемлемым элементом обеспечения частной жизни в цифровом мире. Развитие и распространение конечного шифрования будут иметь важное значение для обеспечения безопасности и конфиденциальности данных в будущем.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический

журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.
8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Куликов А.А., Горелкин А.С., Нефедов А.А. Разработка мобильных приложений на базе ОС IOS с внедрением COREML технологий // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 60–70

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.9

РАЗРАБОТКА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА БАЗЕ ОС IOS С ВНЕДРЕНИЕМ COREML ТЕХНОЛОГИЙ

Куликов А.А., [1]Горелкин А.С., Нефедов А.А.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: [1]gorelk12222@bk.ru

В статье рассматривается ситуация на рынке внедрения и применения искусственного интеллекта при разработке мобильных приложений. Дается обзор современных инструментов и фреймворков, предназначенных для упрощения процесса интеграции и работы с моделями машинного обучения в iOS-приложениях. Целью данной работы является изучение основных принципов разработки приложений для iOS с интеграцией CoreML в мобильные приложения, включая описание основных возможностей, подготовки и обработки данных для моделей машинного обучения, а также создание и обучение таких моделей. Также рассматривается метод тестирования моделей машинного обучения, а также приводятся заключительные выводы исследования.

Ключевые слова: IOS, CoreML, мобильное приложение, машинное обучение, методы тестирования моделей, SwiftUI.

DEVELOPMENT OF MOBILE APPLICATIONS BASED ON IOS WITH THE INTRODUCTION OF COREML TECHNOLOGIES

Kulikov A.A., [1] Gorelkin A.S., Nefedov A.A.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: [1]gorelk12222@bk.ru

The article examines the situation on the market of the introduction and application of artificial intelligence in the development of mobile applications. An overview of modern tools and frameworks designed to simplify the process of integration and working with machine learning models in iOS applications is given. The purpose of this work is to study the basic principles of developing applications for iOS with CoreML integration into mobile applications, including a description of the main features, preparation and processing of data for machine learning models, as well as the creation and training of such models. The method of testing machine learning models is also considered, and the final conclusions of the study are presented.

Keywords: IOS, CoreML, mobile application, machine learning, model testing methods, SwiftUI.

1. Основы разработки мобильных приложений под iOS

Разработка мобильных приложений под iOS [1] требует знания основных принципов и инструментов. Для начала разработки приложений под iOS необходимо изучить язык программирования Swift, который широко используется для создания приложений для этой ОС. Также важно ознакомиться с основным инструментом разработки - Xcode, интегрированной средой разработки, которая предоставляет набор инструментов для создания, отладки и тестирования приложений. При разработке пользовательского

интерфейса необходимо использовать подходы, основанные на готовых компонентах и элементах управления, чтобы обеспечить удобство использования приложения. Анализ подходов для реализации пользовательского интерфейса позволит выбрать наиболее подходящий способ создания интерактивных и интуитивно понятных экранов приложения.

1.1. Анализ подходов для реализации пользовательского интерфейса

Анализ подходов для реализации пользовательского интерфейса является важным этапом разработки мобильных приложений под iOS. Имеется несколько основных подходов, из которых разработчики могут выбрать в соответствии с требованиями проекта: UIKit и SwiftUI [3].

Сравнительный анализ UIKit и SwiftUI

UIKit и SwiftUI являются двумя разными фреймворками для разработки приложений пользовательских интерфейсов в iOS. Главное отличие между ними заключается в подходе к построению пользовательского интерфейса. UIKit использует императивный подход, где разработчику нужно явно указывать каждый шаг при создании интерфейса. В то время как SwiftUI предлагает декларативный подход, где разработчик описывает желаемый интерфейс, и система сама заботится о его построении. Это позволяет сократить количество кода и упростить процесс создания интерфейса в SwiftUI. Сравнительный анализ UIKit и SwiftUI представлен в Таблице 1.

Таблица 1 – Анализ UIKit и SwiftUI

	SwiftUI	UIKit
Скорость вёрстки	+	-
Совместимость с легаси-кодом	-	+
Дебаггинг	-	+
Мультиплатформенность	+	-
Поддержка сообщества	-	+
Количество кода	+	-
Совместимость с Modern Concurrency	+	-
Поддерживаемость	-	+
Быстродействие	+	-

В итоге, выбор между UIKit и SwiftUI зависит от конкретного проекта и предпочтений команды разработчиков.

1.2. Сравнительный анализ архитектурных решений

Архитектура мобильных приложений на iOS представляет собой структурную основу, определяющую организацию кода, разделение обязанностей и взаимодействие компонентов приложения. Архитектурные шаблоны, такие как MVC, MVP, MVVM и VIPER [4], предоставляют разработчикам инструменты для организации кода, управления зависимостями и обеспечения легкости поддержки и масштабируемости приложения.

Сравнительный анализ MVC, MVVM, MVP, VIPER представлен в Таблице 2.

Таблица 2 – Анализ MVC, MVVM, MVP и VIPER

	MVC	MVP	MVVM	VIPER
Разделение ответственности	Неявное разделение ответственности, часто приводит к "толстым" контроллерам и увеличению связности	Presenter отвечает за бизнес-логику и обработку событий, что упрощает тестирование и поддержку	ViewModel управляет предоставлением данных для отображения, что позволяет легче тестировать и поддерживать приложение	Каждый компонент имеет четко определенные обязанности, что упрощает понимание и поддержку кода
Тестирование	Тестирование может быть затруднено из-за сильной связности между компонентами и отсутствия четкого разделения ответственности	Улучшенное тестирование благодаря вынесению логики из View в Presenter	Улучшенное тестирование за счет отделения логики отображения от бизнес-логики в ViewModel	Улучшенная тестируемость за счет отдельных компонентов и четкого разделения ответственности
Расширяемость	Масштабирование и расширение может быть затруднено из-за высокой связности и "толстых" контроллеров	Высокая расширяемость благодаря отделению представления от логики в Presenter	Улучшенная расширяемость и масштабируемость благодаря четкому разделению ответственности и декларативному связыванию данных	Высокая расширяемость за счет отдельных компонентов и четкого разделения ответственности
Сложность	Простота и легкость понимания, но возможно возникновение проблем при масштабировании	Сложность управления большим количеством Presenter и взаимосвязей между ними	Увеличение сложности приложения из-за дополнительных слоев ViewModel и дополнительных механизмов связи	Увеличение сложности проекта из-за большого количества слоев и взаимодействий между ними
Популярность	Широко используется и понятен многим разработчикам, особенно в начале карьеры	Популярен в некоторых областях, но не так широко распространен, как MVC	Пользуется популярностью, особенно в средних и больших проектах	Используется в некоторых проектах, но не так широко распространен, как MVC или MVVM

Каждый из архитектурных подходов имеет свои достоинства и недостатки, которые могут варьироваться в зависимости от конкретного проекта и команды разработчиков.

2. Внедрение технологии CoreML в мобильное приложение для iOS

CoreML [5] — это новая технология, представленная в iOS 11. Она является важным и преобладающим достижением в разработке приложений. CoreML позволяет разработчикам интегрировать модель машинного обучения в приложение для iPhone или iPad.

Основная идея CoreML заключается в том, чтобы облегчить разработчикам интеграцию моделей машинного обучения в приложения. Хотя iOS предлагает и другие способы интеграции машинного обучения, например, использование Python и последующая конвертация модели в формат, совместимый с iOS, CoreML дает множество преимуществ. Например, он оптимизирован для повышения энергоэффективности. Это очень важно для мобильных устройств, поскольку мы хотим максимально эффективно использовать ограниченный заряд батареи.

Причина, по которой CoreML может достичь этого, заключается в том, что для выполнения вычислений машинного обучения в нем используются шейдеры Metal Performance Shaders. Эти шейдеры высоко оптимизированы и работают на GPU. Помимо энергоэффективности, CoreML также обеспечивает очень простой и удобный процесс разработки.

2.1 Инициализация проекта

Чтобы можно было воспользоваться CoreML необходимо обучить модель нейронной сети. Компания Apple представила новый инструмент для работы с моделями в 2019 году под название CreateML [6]. Стартовая страница CreateML представлена на Рисунке 1.

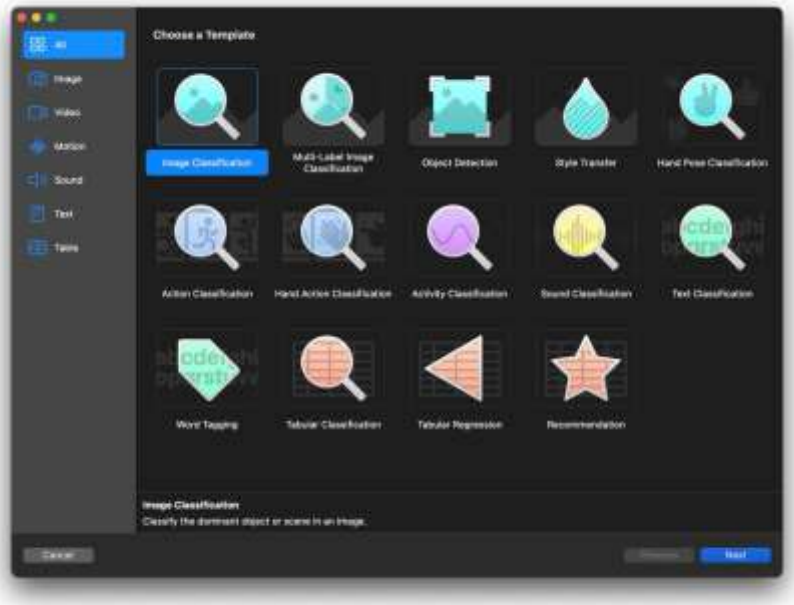

Рисунок 1 – Стартовый экран CreateML

На данный момент CreateML предоставляет возможность обучения на 6 типах данных и 14 шаблонах модели.

При обучении с использованием изображение доступны 5 шаблонов:

- Image Classification. Этот шаблон необходим для задач классификации изображений, где модель должна определить, к какому классу или категории принадлежит данное изображение. Например, классификация фотографий по типу животных, распознавание рукописных цифр и т. д.
- Multi-Label Image Classsification. В отличие от обычной классификации изображений, этот шаблон позволяет присваивать несколько меток или классов одному изображению. Это полезно, когда на изображении присутствуют различные объекты, которые могут быть классифицированы по разным категориям.
- Object Detection. Данный шаблон используется для обнаружения и локализации объектов на изображении. Он определяет прямоугольные области, где находятся объекты, и классифицирует их, позволяя модели точно определять и различать объекты на изображениях.
- Style Transfer. Этот шаблон позволяет переносить стиль одного изображения на другое, создавая новое изображение с сохранением содержания и характеристик первого изображения, но со стилем второго. Это позволяет создавать уникальные художественные эффекты и стилизованные изображения.
- Hand Pose Classification. Данный шаблон необходим для определения позы рук на изображениях. Это полезно для решения задач, связанных с анализом жестов, управлением интерфейсами с помощью жестов или виртуальной реальности.

При обучении с использованием видео доступно 3 шаблона:

- Style Transfer.
- Action Classification. Этот шаблон используется для классификации действий в видео. Он позволяет модели определять различные виды действий, происходящих в видеопотоке, что полезно для мониторинга видеонаблюдения, анализа деятельности и т. д.
- Hand Action Classification. Аналогично шаблону "Action Classification", но специализирован для классификации действий, связанных с движениями рук. Это может быть полезно для систем управления жестами или для анализа движений рук в реальном времени.

Для работы с активностью представлен лишь 1 шаблон:

- Activity Classification. Этот шаблон применяется для классификации общих активностей или событий в видеопотоке. Например, определение, происходит ли на видео ходьба, бег, игра в футбол и т. д. Это полезно для видеоаналитики и мониторинга поведения людей.

Также, как и с активностью, при работе со звуками доступен лишь один шаблон, а именно:

- Sound Classification. Данный шаблон используется для классификации звуковых сигналов. Например, определение типа звука (речь, музыка, шум), распознавание ключевых слов в аудиозаписи и т. д. Это полезно для систем анализа аудиоданных и обработки речи.

Для работы с текстом представлены 2 шаблона:

- Text Classification. Этот шаблон необходим для классификации текстов по определенным категориям или меткам. Например, определение темы новостной

статьи, классификация отзывов на продукты по тональности и т. д. Это полезно для автоматической обработки и анализа текстовой информации.

- Word Tagging. Данный шаблон позволяет размечать отдельные слова или токены в тексте с присвоением им соответствующих меток или категорий. Это помогает в семантическом анализе текста и его понимании компьютером.

Также для работы с таблицами предсталены 3 шаблона:

- Tabular Classification. Этот шаблон используется для классификации данных, представленных в табличной форме, по определенным категориям или меткам. Например, классификация клиентов по их покупательским предпочтениям или определение категории риска в финансовых операциях.
- Tabular Regression. Схож с классификацией, но вместо присваивания категорий предсказывает непрерывные значения для каждого объекта. Например, предсказание цены недвижимости на основе ее характеристик.
- Recommendation. Этот шаблон используется для предсказания предпочтений пользователей или рекомендации контента на основе их предыдущих действий или интересов. Это полезно для создания персонализированных рекомендательных систем в различных приложениях и сервисах.

Инициализируем проект и переходим к обучению. Выберем тип данных изображение и шаблон Image Classification. Экран инициализации проекта CreateML и экран обучения модели нейронной сети представлены на Рисунках 2-3.

Рисунок 2 – Экран инициализации проекта CreateML.

Рисунок 3 – Экран обучения модели нейронной сети

2.2 Подготовка и разметка данных

Следующий важный шаг после создания проекта - подготовка данных, необходимых для обучения модели машинного обучения. Обучающие данные обычно состоят из набора пар вход-выход. Обучающие данные используются для обучения модели машинного обучения, а тестовые - для проверки точности модели. Обычно данные разбиваются случайным образом, при этом значительная часть данных, например 70-80 %, используется для обучения, а оставшаяся часть - для тестирования.

Обучающие данные должны быть в формате, который распознается моделью, используемой для обучения. Структура и формат файлов для Image Classification представлены на Рисунке 4.

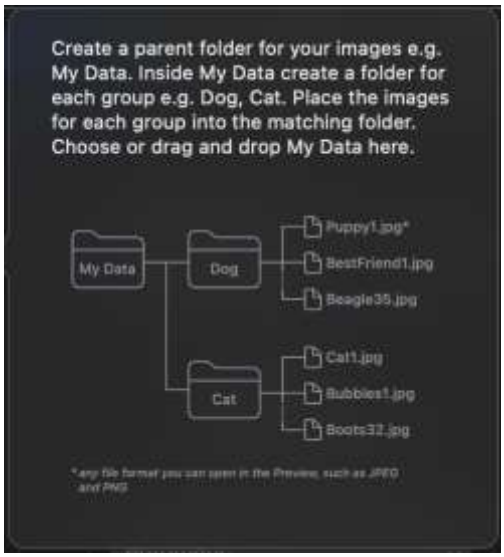

Рисунок 4 – Структура и формат данных для Image Classification

2.3 Обучение нейронной сети

После разметки данных и их импорта в проект необходимо выставить Parameters. Результаты загрузки данных в проект представлены на Рисунке 5.

Рисунок 5 – Результаты загрузки данных в проект

1. Feature extraction или превращение данных, специфических для предметной области, в понятные для модели векторы. Их доступно 2 на выбор:

- Image Feature Print V1 – модель извлечения объектов масштабирует входное изображение до 299 x 299 и выдает размер встраиваемого объекта 2048. Доступно на более старых версиях iOS
- Image Feature Print V2 - Модель извлечения объектов масштабирует входное изображение до 360 x 360 и выдает размер встраиваемого объекта 768. Доступно только с iOS 17

2. Iteration (Итерация):

Это количество повторений обучения, через которые проходят данные. Чем больше итераций, тем больше возможности для модели улучшить свои предсказания, но это также может привести к переобучению модели на обучающих данных.

3. Augmentations (доп. Настройки)

- Add noise (Добавить шум)
- Blur (Размытие)
- Crop (Обрезка)
- Expose (Экспозиция)
- Flip (Отражение)
- Rotate (Поворот)

Так как в iOS разработке принято поддерживать на 2 версии ОС меньше, то оставим Image Feature Print V1. Для более точного предсказания выставим 500 итераций и не будем добавлять другие эффекта.

Запустим обучения с помощью кнопки Train. Результаты обучения модели нейронной сети представлены на Рисунке 6.

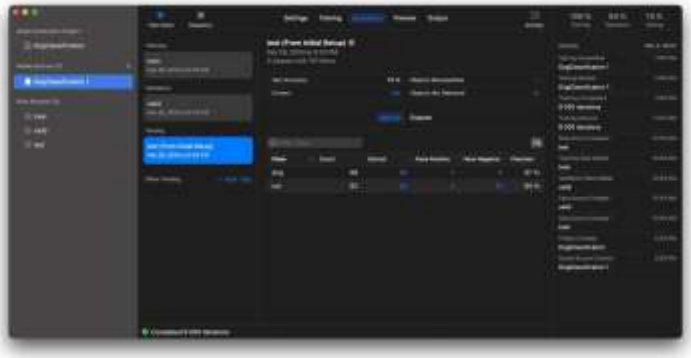

Рисунок 6 – Результаты обучения модели нейронной сети

2.4 Интеграция модели нейронной сети в iOS приложение.

Для начала создадим тестовый проект для проверки нейронной сети в IDE XCode. В качестве архитектурного подхода будем использовать MVC, а для реализации функционала и интерфейса UIKit.

Перенесем нашу созданную модель в проект и проверим ее настройки. Структура проекта и настройки модели представлены на Рисунке 7.

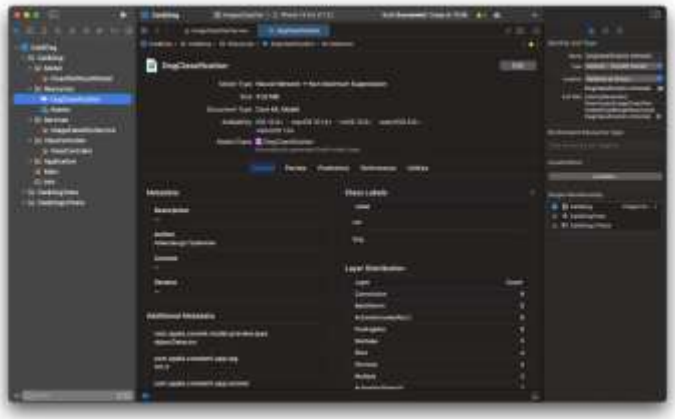

Рисунок 7 – Структура проекта и настройки модели

Следующим шагом реализуем контроллер, который будет брать изображение и прогонять его через классификатор, чтобы на выходе получить распознанный объект. Затем проверим его работоспособность на реальных тест-кейсах.

2.5 Тестирование нейронной сети

Тестирование можно производить двумя способами [6]. А именно:

- В самом приложение CreateML
- На мобильном устройстве или эмуляторе.

Мы будет тестировать вручную на реальном устройстве. Результаты тестирования представлены на Рисунке 8.

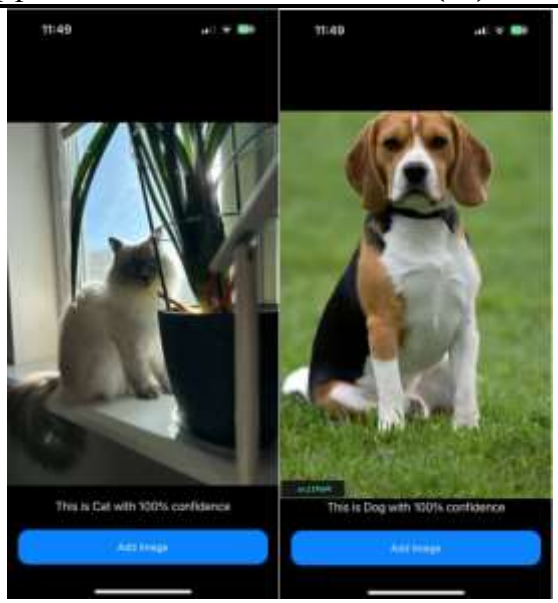

Рисунок 8 – Результаты тестирования

Как можно увидеть, в результате тестирования модель нейронной сети успешно классифицирует объекты на изображении с вероятностью 100%.

Результаты исследования

Исследование позволило выявить основные моменты, связанные с разработкой мобильных приложений на базе ОС iOS с внедрением CoreML технологий. Были освещены основы разработки мобильных приложений на iOS. Также были проанализированы возможности интеграции CoreML в мобильные приложения, включая подготовку и обработку данных для моделей машинного обучения, а также создание и тренировку самих моделей. Также были представлены методы тестирования моделей машинного обучения при интеграции CoreML.

Список литературы

1. Ларионов Д.А. Мобильное приложение на основе iOS. Москва: "ГелиосАРТ", 2017.
2. Императивный UIKit vs Декларативный SwiftUI - 2023, https://habr.com/ru/companies/ozontech/articles/742750/
3. Raúl Ferrer García. iOS Architecture Patterns: MVP, MVVM, VIPER, and VIP in Swift. - 2023, C.397.
4. Дьяков А.В., Наумова Е.А. Машинное обучение на языке Swift с использованием CoreML. Москва: "LRF Media", 2021.
5. Create ML. Create machine learning models for use in your app. – 2024, https://developer.apple.com/documentation/createml
6. Avi Tsadok. Pro iOS Testing – 2020, C.320.

References

1. Larionov D.A. Mobile application based on iOS. Moscow: HeliosART, 2017.
2. Imperative UIKit vs Declarative Swiftai - 2023, https://habr.com/ru/companies/ozontech/articles/742750/

3. Paul Ferrer Garcia. iOS Architecture Patterns: MVC, MVVM, VIPER, and VIP in Swift. - 2023, pp.397.
4. Dyakov A.V., Naumova E.A. Machine learning in Swift using Corel. Moscow: LRF Media, 2021.
5. Create ML. Create machine learning models for use in your app. – 2024, https://developer.apple.com/documentation/createml
6. Avi Tsadok. Pro iOS Testing – 2020, pp.320.

Шабуня В.В. и др. Анализ развития квантовых технологий в интересах криптографии, связи и навигации/ Шабуня В.В., Лукашев А.В., Якушенко С.А., Селезнев А.В. // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 71–76

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 530.145

АНАЛИЗ РАЗВИТИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ В ИНТЕРЕСАХ КРИПТОГРАФИИ, СВЯЗИ И НАВИГАЦИИ

[1]Шабуня В.В., [2]Лукашев А.В., Якушенко С.А., Селезнев А.В.
ФГКОУ ВО «ВОЕННАЯ ОРДЕНОВ ЖУКОВА И ЛЕНИНА КРАСНОЗНАМЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С.М.БУДЕННОГО" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, Санкт-Петербург, Россия, (194064, Санкт-Петербург, Тихорецкий пр-кт, д.3), e-mail: [1]vvsch1970@mail.ru, [2]lukasheff@mail.ru

Рассмотрены основные тенденции развития квантовых коммуникаций. Показано, что применение квантового ключа дает существенные преимущества перед другими способами криптографии, что делает его весьма привлекательными в качестве базовой инфраструктуры безопасности телекоммуникаций в целом.

Ключевые слова: Квантовые технологии, квантовые сети, квантовое распределение ключей, источники одиночных фотонов.

ANALYSIS OF THE DEVELOPMENT OF QUANTUM TECHNOLOGIES IN THE INTERESTS OF CRYPTOGRAPHY, COMMUNICATION AND NAVIGATION

Shabunya V.V., Lukashev A.V., Yakushenko S.A., Seleznev A.V.
MILITARY ORDER OF ZHUKOV AND LENIN RED BANNER ACADEMY OF COMMUNICATIONS NAMED AFTER MARSHAL OF THE SOVIET UNION S.M. BUDYONNY OF THE MINISTRY OF DEFENSE OF THE RUSSIAN FEDERATION, St. Petersburg, Russia, (194064, St. Petersburg, Tikhoretsky pr-kt, 3), e-mail: [1]vvsch1970@mail.ru, [2]lukasheff@mail.ru

The main trends in the development of quantum communications are considered. It is shown that the use of a quantum key provides significant advantages over other methods of cryptography, which makes it very attractive as a basic telecommunications security infrastructure in general.

Keywords: Quantum technologies, quantum networks, multi-core fiber, quantum key distribution, single photon sources.

Квантовые технологии нового поколения используют известную квантовую физику, но развиваются феноменальными темпами, что в основном обусловлено коммерческими интересами. Однако, в сфере обороны и безопасности по ключевым направлениям, таким как связь, вычислительная техника, позиционирование, навигация и синхронизация, зондирование, развиваются неравномерно. Публикации совсем недавнего времени говорили о ближайшем горизонте развития квантовых технологий в более чем 20 лет, однако европейское международное сотрудничество ускоряет прогресс. В нашем же случае, опора может быть только на отечественные технологии. Разработки в области квантовых технологий

оцениваются как перспективные, при этом требующие уже не так много времени (от 5 до 10 лет), прежде чем их прорывной характер полноценно проявится в отношении военного потенциала. Большие данные с элементами квантовой обработки информации значительно ускорят возможности сбора, обработки, хранения, поиска и непосредственно использования. Поэтому основные направления разработок в ближайшей перспективе – защита информации по принципу квантового распределения ключей (далее – КРК), прямая безопасная связь, потоковое шифрование, стеганография и цифровая подпись [1, 2].

Однако, как показали специальные исследования [3] простое сопряжение разных устройств не позволяет реализовать устойчивое распределение квантовых ключей с необходимой для практических приложений скоростью. Реализация КРК становится возможной после определенной доработки терминалов и модификации алгоритмов синхронизации.

В настоящее время появляется второе поколение квантовых технологий, способных создавать и использовать более сложные и тонкие аспекты квантовой физики. Эффективно реализуются стеки протоколов квантовой прямой безопасной связи или сетевой связи на доверенных узлах. Более глубокое взаимодействие передового производства, материаловедения и накопления энергии позволяет на порядок повысить вычислительные возможности, которые будут выходить за теоретические пределы классических компьютеров для конкретных классов аналитических задач. Развитие криптографии в целом ведет к способности расшифровывать закодированные сообщения с использованием современных криптографических методов, что окажет революционное воздействие на современные системы связи. В период 2025 – 2040 годов основную угрозу, по мнению военных экспертов НАТО, несут новые методы шифрования, возможная потеря воздушной и подводной скрытности, а также потенциальное преимущество противника в создании аналитических систем для поддержки принятия решений, обеспечиваемых квантовыми вычислениями [4]. Тем более, что современный уровень науки и техники, а также доступность систем программно-управляемого радио в совокупности с вычислительными мощностями, позволяют эффективно находить уязвимости в реализованных решениях и успешно производить различные деструктивные действия с эксплуатируемыми системами и комплексами. Использование же квантовых технологий сопряжено со значительными проблемами интероперабельности, и как следствие, соображениями национальной безопасности. Также сдерживающим фактором является высокий уровень математической сложности и необходимые в таких случаях огромные инвестиции в НИОКР, с соответствующими финансовыми рисками. Следует отметить следующие направления исследований (Таблица 1):

Таблица 1 – Области исследований квантовых технологий

Технологическая область	Воздействие	Уровень готовности технологий	Временной горизонт
Связь	Высокое	Проверка опытных образцов в реальных условиях	2035-2040
Информатика	Революционное	Проверка опытных образцов в лабораторных условиях	2030-2035

Технологическая область	Воздействие	Уровень готовности технологий	Временной горизонт
Точная навигация	Высокое	Демонстрация прототипов в реальных условиях	2025-2030
Датчики	Умеренное	Аналитическое и экспериментальное доказательство концепции	2030-2035

Квантовая связь – область исследований не только в коммерческих интересах, но и военных. В краткосрочной перспективе с помощью квантовых технологий возможно обнаружение подслушивающих устройство на канале связи. В среднесрочной перспективе сосредоточение будет происходить на оптической квантовой связи для защиты от подслушивания и в качестве защиты от помех. В долгосрочной перспективе – разработка глобальной распределенной квантовой системы для поддержки защищенной связи.

Квантовые вычисления – область исследований и разработки подлинного универсального квантового компьютера общего назначения. В среднесрочной перспективе разработка новых квантово-оптимизированных алгоритмов для ограниченных задач.

Квантовое моделирование – область исследований с прогнозированием характеристик материалов, что позволит использовать проектирование новых с определенными желательными физическими свойствами, такими как сверхпроводимость, устойчивость к агрессивным средам с высокими характеристиками.

Позиционирование, навигация и синхронизация включает передачу и прием внешних сигналов, таких как GPS, а другой опирается на автономное восприятие движения, например, обеспечиваемое инерциальными системами. Квантовые технологии поддержат сочетание сверхточных измерений времени со сверхточными измерениями ускорения и углового вращения, чтобы обеспечить сверхточную инерциальную навигацию и синхронизацию.

Квантовое дистанционное зондирование – такое зондирование, которое обладает потенциалом сделать стелс-технологии устаревшими, обеспечить более точную идентификацию целей, скрытое обнаружение и наблюдение. Прототипом считается квантовый радар. Квантовые датчики позволят проводить гораздо более точные и чувствительные измерения и использовать гораздо меньшую мощность для обнаружения и отслеживания небольших или малозаметных целей.

Магнитное и гравитационное зондирование: точное измерение магнитного поля используется морскими патрульными самолетами для локализации подводных лодок с использованием датчиков магнитных аномалий. Современные датчики не подходят для использования на небольших беспилотных летательных аппаратах из-за ограничений по размеру, весу и мощности, но новые квантовые технологии могут обеспечить решение этой проблемы. Существуют также специальные технологии гравитационного зондирования, которые могут быть использованы, например, для навигации подводных аппаратов [5].

Акцентируя внимание на технологии КРК, необходимо отметить, что данные системы потенциально интересны для ряда узкоспециализированных применений: обеспечение ключами линейных систем защиты информации между узлами волоконно-оптической сети; обеспечение ключами с целью шифрования трафика космических радиолиний; обеспечение

ключами абонентских устройств телефонной, видеосвязи, передачи данных при их взаимодействии через один сервер в рамках пункта управления с целью повышения защищенности информации от перехвата в рамках контролируемой зоны и снижения требований к абонентским линиям; обеспечение ключами на наиболее значимых информационных направлениях в режиме «одноразового блокнота»; обеспечение ключами на труднодоступных автономных объектах; усиление стойкости криптосистем [6].

Интеграция квантовой криптографической системы с выработкой и распределения ключей позволит уменьшить ресурсную нагрузку на ключевую систему в случае компрометации части абонентов сети, а также исключит дополнительные временные задержки, связанные с подготовкой систем. А использование в интересах интернета вещей (интернета боевых вещей) с целью организации мульти-платформенной поддержки вариаций, взаимодействующих между собой систем, предлагается использование готового базиса [7].

Рисунок 1 – Схема интеграции квантовых коммуникаций в инфраструктуру управления сетью интернета вещей

Рисунок 2 – Схема интеграции квантовых коммуникаций в инфраструктуру управления сетью интернета вещей

В каждом конкретном случае необходимо принимать решение после проведения анализа преимуществ, при этом усилия по совершенствованию рекомендуется сосредоточить на повышении эксплуатационных и экономических показателей, т.е. с технико-экономическим обоснованием относительно альтернативных способов обеспечения требуемой стойкости криптосистем к квантовым атакам. Хотя новые квантовые технологии обладают потенциалом революционного воздействия при их использовании в военных целях, большинство из них находятся на ранних стадиях развития, и до глобального внедрения предстоит решить серьезные технические задачи.

Список литературы

1. Кулик С.П. Квантовые технологии: современное состояние и перспективы// Наноиндустрия. 2020. – Т. 13, № S4(99). – С. 702. – DOI 10.22184/1993-8578.2020.13.4s.702.
2. Морозов О.Г., Нуреев И.И., Сахабутдинов А.Ж., Мисбахов Р.Ш. Кузнецов А.А. Приоритет 2030: Новые направления научных исследований кафедры радиофотоники и микроволновых технологий//Киберфизические системы | Электроника, фотоника и киберфизические системы. 2021. Т. 1. № 2. С. 45–58.
3. Лукашев А. В., Шабуня В. В. и др. Квантовые технологии в системах связи специального назначения: информационно-аналитический обзор. – СПБ: ПОЛИТЕХ-ПРЕСС, 2023, – 165 с.
4. «Характеристики систем и средств связи ведущих зарубежных стран на период до 2035 года». ФГКУ «ЦИВПЗС» МО РФ. Выпуск № 2330, М., 2019.
5. Лукашев А.В., Шабуня В.В., Полищук В.Р., Билан В.В. Квантовые технологии. Тенденции повышения уязвимости современных систем информационного обмена. Стр. 102-114. Международная научно-практическая конференция «Военная связь будущего. Квантовый скачок как неизбежность»: Сборник материалов. СПб.: ВАС, 2023. – 276 с.
6. Полищук В.Р., Лукашев А.В., Шабуня В.В., Федоров Д.И. Квантовая криптография: физические основы, протоколы, перспективы применения в системах связи специального назначения. С. 127-137. Международная научно-практическая конференция «Военная связь будущего. Квантовый скачок как неизбежность»: Сборник материалов. СПб.: ВАС, 2023. – 276 с.
7. Чеусов С.С. Перспективы интегрирования квантовых технологий в систему управления средствами огневого поражения. С. 42-47. Международная научно-практическая конференция «Военная связь будущего. Квантовый скачок как неизбежность»: Сборник материалов. СПб.: ВАС, 2023. – 276 с.

References

1. Kulik S.P. Quantum technologies: current state and prospects// Nanoindustry. 2020. – Vol. 13, No. S4(99). – p. 702. – DOI 10.22184/1993- 8578.2020.13.4 s.702.

2. Morozov O.G., Nureyev I.I., Sahabutdinov A.J., Misbakhov R.S. Kuznetsov A.A. Priority 2030: New directions of scientific research of the Department of Radiophotonics and Microwave Technologies // Cyberphysical systems | Electronics, photonics and cyberphysical systems. 2021. Vol. 1. No. 2. pp. 45-58.
3. Lukashev A.V., Shabunya V. V. and others. Quantum technologies in special-purpose communication systems: an information and analytical review. – St. Petersburg: POLYTECH PRESS, 2023, p.165
4. "Characteristics of communication systems and means of leading foreign countries for the period up to 2035". FGKU "TSIVPZS" OF THE Ministry OF Defense OF THE Russian Federation. Issue No. 2330, Moscow, 2019.
5. Lukashev A.V., Shabunya V.V., Polishchuk V.R., Bilan V.V. Quantum technologies. Trends in increasing vulnerability of modern information exchange systems. pp. 102-114. International scientific and practical conference "Military communications of the future. Quantum leap as an inevitability": Collection of materials. St. Petersburg: VAS, 2023. – p.276
6. Polishchuk V.R., Lukashev A.V., Shabunya V.V., Fedorov D.I. Quantum cryptography: physical foundations, protocols, prospects of application in special-purpose communication systems. pp. 127-137. International scientific and practical conference "Military communications of the future. Quantum leap as an inevitability": Collection of materials. St. Petersburg: VAS, 2023. – 276 p.
7. Cheusov S.S. Prospects for integrating quantum technologies into the fire damage control system. pp. 42-47. International scientific and practical conference "Military communications of the future. Quantum leap as an inevitability": Collection of materials. St. Petersburg: VAS, 2023. – p.276

Перевертун Д.Р. Методы аутентификации и управления доступом
// Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 77–84

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.05

МЕТОДЫ АУТЕНТИФИКАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

В эпоху быстрого развития цифровых технологий и увеличения объемов конфиденциальной информации, хранящейся в электронном виде, вопросы аутентификации и управления доступом приобретают критическую важность. Статья охватывает широкий спектр методов и подходов к аутентификации и управлению доступом, включая традиционные пароли, биометрическую аутентификацию, многофакторную аутентификацию, адаптивную аутентификацию, а также применение децентрализованных идентификаторов и блокчейн технологий. Анализируя каждый из этих методов, статья выявляет их преимущества и недостатки, а также рассматривает потенциальные направления развития в области управления доступом и аутентификации для обеспечения высокого уровня безопасности в цифровом мире.

Ключевые слова: Аутентификация, управление доступом, многофакторная аутентификация, биометрическая аутентификация, децентрализованные идентификаторы, блокчейн, безопасность данных, цифровая идентичность, принцип наименьших привилегий, адаптивная аутентификация.

AUTHENTICATION AND ACCESS CONTROL METHODS

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

In an era of rapid development of digital technologies and an increase in the volume of confidential information stored electronically, authentication and access control issues are becoming critically important. The article covers a wide range of methods and approaches to authentication and access control, including traditional passwords, biometric authentication, multi-factor authentication, adaptive authentication, as well as the use of decentralized identifiers and blockchain technologies. Analyzing each of these methods, the article identifies their advantages and disadvantages, as well as considers potential development directions in the field of access control and authentication to ensure a high level of security in the digital world.

Keywords: Authentication, access control, multifactor authentication, biometric authentication, decentralized identifiers, blockchain, data security, digital identity, principle of least privilege, adaptive authentication.

В современном мире, где информационные технологии играют ключевую роль в бизнесе, науке и повседневной жизни, вопросы аутентификации и управления доступом становятся все более актуальными. С развитием интернета вещей, облачных вычислений и мобильных технологий, необходимость в надежных методах проверки подлинности и управления доступом к ресурсам никогда не была более острой. Эта статья рассматривает

различные аспекты аутентификации и управления доступом, анализируя современные методы и подходы, их преимущества и недостатки, а также потенциальные направления развития в этой области.

Аутентификация — это процесс верификации идентичности пользователя, при котором система убеждается в том, что пользователь действительно является тем, за кого себя выдает. Управление доступом, в свою очередь, — это процесс, который после аутентификации определяет, к каким ресурсам и операциям пользователь имеет доступ. Эти два процесса тесно связаны, поскольку надежная аутентификация является основой для эффективного управления доступом.

В основе процессов аутентификации и управления доступом лежит идея верификации идентичности пользователя и последующего определения его прав на выполнение определенных действий или доступ к ресурсам. Эти процессы тесно связаны и играют важную роль в обеспечении безопасности информационных систем. Аутентификация представляет собой первый шаг, в ходе которого система должна убедиться, что пользователь или система действительно являются теми, за кого себя выдают.[6] Этот процесс можно сравнить с предъявлением документа, удостоверяющего личность, при входе в защищенное здание. Как только идентичность подтверждена, наступает этап управления доступом, который определяет, какие действия или ресурсы доступны пользователю на основе его прав и ролей в системе.

Этот механизм не просто черно-белый фильтр, пропускающий внутрь всех, кто успешно прошел аутентификацию; он более тонко настраивает уровень доступа каждого пользователя, гарантируя, что каждый имеет доступ только к тем ресурсам, которые необходимы для выполнения своих задач.[3] Так, например, сотрудник службы поддержки может иметь доступ к базе данных обращений пользователей, но не к финансовой информации компании, в то время как у бухгалтера будут права на просмотр и редактирование финансовых документов, но не обращений клиентов.

Важность такого подхода сложно переоценить, поскольку он лежит в основе защиты конфиденциальности и интегритета данных, а также обеспечивает соблюдение нормативных и законодательных требований к защите информации.[1] Именно благодаря грамотно построенным процессам аутентификации и управления доступом организации способны минимизировать риски несанкционированного доступа к чувствительным данным и поддерживать высокий уровень безопасности информационных систем.

Традиционно, аутентификация осуществляется с помощью чего-то, что пользователь знает (например, пароль), чего-то, что у пользователя есть (например, смарт-карта или токен), или чего-то, что является частью пользователя (биометрия, например отпечатки пальцев). Несмотря на широкое распространение, каждый из этих методов имеет свои недостатки. Пароли могут быть подобраны или украдены, токены потеряны, а биометрические данные скопированы или подделаны.

Традиционные методы аутентификации включают в себя использование паролей, физических устройств, таких как смарт-карты или токены, и биометрических данных, например отпечатков пальцев. Эти методы на протяжении многих лет служили основой для проверки подлинности пользователей, предоставляя различные уровни защиты и удобства. Пароли, вероятно, самый распространенный метод, основанный на знании пользователя уникальной комбинации символов, которую можно ввести для доступа к системе. Однако,

несмотря на их широкое распространение, пароли подвержены множеству угроз, таких как фишинг, подбор пароля и социальная инженерия.

Физические устройства, такие как смарт-карты или токены, представляют собой еще один слой защиты, поскольку требуют от пользователя нечто, что он имеет. Эти устройства могут генерировать одноразовые пароли или использоваться в сочетании с пин-кодом для доступа к ресурсам. Такой подход значительно повышает безопасность, но влечет за собой дополнительные затраты и неудобства, связанные с необходимостью постоянно носить с собой эти устройства.

Биометрическая аутентификация использует уникальные физиологические или поведенческие характеристики человека, такие как отпечатки пальцев, геометрия лица, голос или даже рисунок радужки глаза, как средство идентификации. Биометрия предлагает высокий уровень безопасности и удобства, поскольку пользователям не нужно запоминать сложные пароли или носить с собой дополнительные устройства. Однако этот метод также имеет свои недостатки, включая возможность ошибок при считывании, проблемы с приватностью и потенциальную уязвимость перед биометрическим спуфингом.

В целом, традиционные методы аутентификации предоставляют основу для защиты доступа к системам и данным, но каждый из них имеет свои ограничения и уязвимости. Это подчеркивает необходимость постоянного развития и адаптации методов аутентификации для обеспечения надежной защиты в меняющемся технологическом ландшафте.

В ответ на ограничения традиционных методов развивается многофакторная аутентификация (MFA), которая сочетает два или более метода из разных категорий, значительно увеличивая уровень безопасности. Например, использование пароля в сочетании с одноразовым кодом, отправленным на мобильный телефон пользователя, значительно затрудняет несанкционированный доступ.

Многофакторная аутентификация, или MFA, представляет собой процесс, в котором для подтверждения идентичности пользователя требуется несколько методов аутентификации из разных категорий, что значительно повышает безопасность по сравнению с использованием одного метода. Этот подход основан на предположении, что даже если один из факторов будет скомпрометирован, шансы на то, что злоумышленник сможет обойти все уровни защиты, существенно снижаются. MFA обычно включает комбинацию чего-то, что известно пользователю (например, пароль или пин-код), чего-то, что у пользователя есть (например, смартфон или специальный токен), и чего-то, что является частью пользователя (например, биометрические данные).

Применение MFA начинается с использования традиционного пароля, что уже является стандартной практикой. Однако, в отличие от простой аутентификации по паролю, в процесс добавляется еще один или несколько дополнительных шагов. Это может быть одноразовый код, отправленный на мобильное устройство пользователя посредством SMS или специализированного приложения, или же запрос на подтверждение входа через приложение управления учетными записями. Для еще большей защиты может быть использован биометрический сканер, который проверяет уникальные физиологические характеристики пользователя, такие как отпечаток пальца, геометрия лица или скан радужки глаза.

Таким образом, даже если злоумышленникам удастся узнать или угадать пароль пользователя, без доступа к физическому устройству или биометрическим данным они не смогут получить доступ к защищенной информации. Эта методика особенно ценна в условиях

постоянно растущего числа попыток фишинга и других видов кибератак, направленных на получение конфиденциальных данных пользователя. MFA эффективно укрепляет защиту, минимизируя риски, связанные с утечкой данных и несанкционированным доступом, и является критически важным элементом современной стратегии информационной безопасности.

С развитием технологий биометрическая аутентификация становится все более популярной благодаря своей удобству и высокому уровню безопасности. Современные биометрические системы используют не только отпечатки пальцев, но и распознавание лиц, голоса, радужки глаза и даже поведенческую биометрию, такую как динамика набора текста или образец движения мыши.

Биометрическая аутентификация представляет собой метод верификации идентичности пользователя на основе уникальных физиологических или поведенческих характеристик. В отличие от традиционных подходов, основанных на знании (например, пароли) или владении (например, ключи или карты), биометрическая аутентификация исключает необходимость помнить сложные пароли или носить с собой физические устройства. Этот метод использует уникальные признаки человека, такие как отпечатки пальцев, геометрия лица, сканирование радужки глаза, распознавание голоса или даже уникальные характеристики походки. Благодаря тому, что каждый человек обладает уникальными биометрическими данными, этот метод обеспечивает высокий уровень безопасности и удобства.

Применение биометрической аутентификации охватывает широкий спектр сценариев, от разблокировки смартфонов и ноутбуков до доступа в защищенные зоны и системы. Процесс аутентификации происходит путем сравнения представленных биометрических данных с предварительно сохраненными образцами в базе данных. Если система обнаруживает совпадение, доступ предоставляется.[2] Это не только ускоряет процесс аутентификации, но и значительно повышает его надежность, поскольку подделка биометрических данных значительно сложнее, чем кража пароля или физического токена.

Однако, несмотря на преимущества, биометрическая аутентификация имеет и свои недостатки. Ошибки при считывании данных, изменения биометрических характеристик со временем и потенциальные вопросы конфиденциальности и приватности данных требуют тщательного рассмотрения и адресации. Кроме того, существует риск централизованного хранения биометрических данных, что может стать мишенью для кибератак. Тем не менее, с постоянным развитием технологий и усилениями в области защиты данных, биометрическая аутентификация продолжает зарекомендовать себя как один из самых перспективных и надежных методов проверки подлинности пользователя.

В последнее время блокчейн технологии и децентрализованные идентификаторы начинают активно применяться в сфере аутентификации и управления доступом. Децентрализованные идентификаторы (DID) — это новый тип идентификатора, который позволяет пользователю полностью контролировать свою цифровую идентичность без необходимости полагаться на центральный авторитет. Это означает, что пользователи могут управлять своей идентичностью и данными лично, без посредников. Блокчейн обеспечивает безопасность и непрерывность этого процесса, записывая каждое изменение в распределенный реестр, который практически невозможно подделать или изменить.

В сфере аутентификации и управления доступом наблюдается стремительное развитие децентрализованных идентификаторов и применение блокчейн технологий. Эти инновации

представляют собой переломный момент, изменяя фундаментальные принципы управления цифровой идентичностью и предоставления доступа к ресурсам. Суть децентрализованных идентификаторов заключается в предоставлении пользователю полного контроля над его цифровой идентичностью, что радикально отличается от традиционных подходов, при которых управление идентификаторами осуществляется централизованными ауторитетами, такими как сервисы электронной почты, социальные сети или корпоративные системы.

Блокчейн технологии, служащие основой для децентрализованных идентификаторов, обеспечивают неизменяемость и прозрачность всей системы. Записи о цифровой идентичности пользователя размещаются в блокчейне, обеспечивая высокий уровень безопасности и защиты от подделок, поскольку изменение какой-либо информации в одном блоке потребует изменений во всех последующих блоках, что практически невозможно без обнаружения. Таким образом, блокчейн позволяет создать надежную и прозрачную систему управления идентификаторами, где пользователь может легко подтвердить свою идентичность, не беспокоясь о рисках утечки данных или несанкционированного доступа.

Децентрализованные идентификаторы и блокчейн технологии вносят значительный вклад в улучшение методов аутентификации и управления доступом, предлагая новые возможности для обеспечения приватности и безопасности в цифровом мире. Эти технологии дают пользователю возможность взять управление своей цифровой идентичностью в свои руки, что является значительным шагом вперед по сравнению с традиционными централизованными системами, часто подверженными риску централизованных атак и утечек данных. Применение децентрализованных подходов и блокчейн технологий в аутентификации и управлении доступом открывает новые горизонты для создания более безопасных, удобных и контролируемых пользователем систем идентификации.

Адаптивная аутентификация — это подход, который использует контекстную информацию (например, местоположение, время входа, используемое устройство) для оценки уровня риска каждой попытки доступа и адаптации требований к аутентификации соответственно. Это может включать требование дополнительных факторов аутентификации в ситуациях, когда уровень риска высок, или упрощение процесса аутентификации, когда риск низкий. Адаптивная аутентификация и управление доступом позволяют создать баланс между удобством для пользователя и необходимостью обеспечения безопасности. Адаптивная аутентификация и управление доступом представляют собой передовой подход к обеспечению безопасности, который учитывает динамичность современного цифрового мира. Эта методика отличается от традиционных статичных систем тем, что она анализирует ряд контекстных факторов во время попытки доступа пользователя к ресурсам или системам, позволяя таким образом динамически адаптировать требования к аутентификации. Эти факторы могут включать местоположение пользователя, используемое устройство, время доступа и даже тип запрашиваемых данных или услуг.

Основываясь на анализе этих данных, система может определить уровень риска каждой отдельной попытки доступа и, соответственно, адаптировать механизмы аутентификации. Например, если пользователь пытается получить доступ из известного местоположения в обычное рабочее время с помощью устройства, которое регулярно используется для этих целей, система может снизить требования к аутентификации, сделав процесс входа более удобным. В противоположность, попытка входа с неизвестного устройства или из аномального местоположения может вызвать запрос на дополнительные факторы

аутентификации, такие как код подтверждения, отправленный на доверенное устройство, или даже биометрическую проверку.[4]

Этот интеллектуальный подход позволяет создать баланс между безопасностью и удобством для пользователя, повышая защиту без создания ненужных препятствий для легитимного доступа.[7] Адаптивная аутентификация и управление доступом также способствуют повышению общей безопасности системы, так как они позволяют мгновенно реагировать на подозрительные действия, минимизируя риск несанкционированного доступа и потенциальных угроз.

В эпоху, когда кибератаки становятся все более изощренными, а методы взлома постоянно эволюционируют, адаптивная аутентификация и управление доступом представляют собой ключевые инструменты для защиты цифровых активов. Они обеспечивают организациям гибкость и мощные средства защиты, необходимые для эффективного реагирования на постоянно меняющуюся угрозу безопасности в цифровом пространстве.

Управление доступом играет ключевую роль в предотвращении утечек данных. Разграничение доступа к информационным ресурсам на основе ролей пользователей (RBAC), принцип наименьших привилегий и постоянный мониторинг и аудит действий пользователей — все это помогает минимизировать риск несанкционированного доступа и утечек данных. Эффективное управление доступом требует постоянного пересмотра и обновления политик доступа, чтобы они соответствовали меняющимся бизнес-процессам и угрозам безопасности.

Предотвращение утечки данных является одной из ключевых задач современной информационной безопасности, и управление доступом играет в этом процессе важнейшую роль. Эффективное управление доступом обеспечивает, чтобы каждый пользователь или система имели доступ только к тем данным и ресурсам, которые необходимы для выполнения их задач, тем самым снижая риск несанкционированного доступа к чувствительной информации.

В основе этого подхода лежит принцип наименьших привилегий, который предполагает предоставление пользователям минимально возможных прав и доступа, необходимых для их работы.[5] Это означает, что доступ к информации строго контролируется и ограничивается в соответствии с ролями и обязанностями пользователя в организации. Такой подход позволяет не только минимизировать возможности для утечки данных, но и упростить отслеживание и анализ действий пользователей в системе, что важно для выявления и предотвращения потенциальных угроз.

Кроме того, управление доступом включает в себя механизмы аутентификации и авторизации, которые гарантируют, что доступ к ресурсам получают только те пользователи, которые прошли надлежащую проверку и которым этот доступ явно разрешен. Эти механизмы могут включать в себя как традиционные методы, такие как пароли и PIN-коды, так и более современные, например многофакторную аутентификацию и биометрическую верификацию.

Для обеспечения долгосрочной защиты данных управление доступом должно быть динамичным и адаптироваться к изменениям в организационной структуре и технологическом ландшафте. Это включает в себя регулярный пересмотр и корректировку политик доступа, а также мониторинг и аудит системы на предмет аномальных действий, которые могут указывать на попытки несанкционированного доступа или внутренние угрозы.

Таким образом, управление доступом выступает в качестве многоуровневой защиты от утечки данных, сочетая в себе строгий контроль над правами доступа, продвинутые методы аутентификации и постоянный анализ действий пользователей. Эти меры, применяемые совместно, создают надежный барьер для защиты ценной информации организации от внешних и внутренних угроз.

В заключение, обеспечение безопасности в современном цифровом мире требует комплексного подхода к аутентификации и управлению доступом. Развитие технологий и появление новых угроз делают эти процессы не только актуальными, но и необходимыми для защиты цифровых активов и конфиденциальной информации. Мы рассмотрели различные аспекты аутентификации и управления доступом, начиная от традиционных методов, таких как использование паролей и биометрических данных, до современных подходов, включая многофакторную аутентификацию, адаптивную аутентификацию, а также применение децентрализованных идентификаторов и блокчейн технологий.

Важность адаптации к новым технологиям и методикам обеспечения безопасности не может быть переоценена. Управление доступом и аутентификация являются критически важными компонентами защиты информации, которые помогают предотвращать несанкционированный доступ и утечку данных. Эффективная реализация этих процессов требует постоянного пересмотра и обновления, чтобы соответствовать меняющимся условиям и угрозам безопасности.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.

Мокряк А.В. и др. Расширенная реальность/Муленко М.Д., Лескова Д.О., Сафонова Т.В., Мокряк А.В.// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 85–91

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.67

РАСШИРЕННАЯ РЕАЛЬНОСТЬ

Муленко М.Д., Лескова Д.О., Сафонова Т.В., [1]Мокряк А.В.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79)
[1]ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

Расширенная реальность — это новая технология, которая позволяет нам видеть и взаимодействовать с цифровыми объектами в нашем реальном мире, Она объединяет виртуальные объекты и информацию с реальным окружением пользователя, обогащая его с помощью компьютерной графики, звука, видео и других сенсорных данных. В отличие от виртуальной реальности, где пользователь полностью погружается в виртуальное пространство, в расширенной реальности виртуальные элементы добавляются к окружающей действительности. В этой статье мы рассмотрим, что такое расширенная реальность, применение её в различных отраслях, преимущества и проблемы данной технологии, а также её будущие перспективы развития. Данная статья поможет понять, что такое расширенная реальность и как она может изменить повседневную жизнь.

Ключевые слова: Расширенная реальность, виртуальная реальность, дополненная реальность, смешанная реальность.

AUGMENTED REALITY

Mulenko M.D., Leskova D.O., Safonova T.V., [1]Mokryak A.V.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79)
[1]ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt,149), e-mail: [1]mokryakanna@mail.ru

Augmented reality is a new technology that allows us to see and interact with digital objects in our real world, It combines virtual objects and information with the user's real environment, enriching it with computer graphics, sound, video and other sensory data. Unlike virtual reality, where the user is completely immersed in a virtual space, in augmented reality, virtual elements are added to the surrounding reality. In this article, we will look at what augmented reality is, its application in various industries, the advantages and problems of this technology,

as well as its future development prospects. This article will help you understand what augmented reality is and how it can change everyday life.

Keywords: Augmented reality, virtual reality, augmented reality, mixed reality.

Введение

В наше время, в эпоху стремительного технологического прогресса, важно быть в курсе последних инноваций и использовать их в своей работе, бизнесе или повседневной жизни. Расширенная реальность — это технология, которая позволяет добавлять виртуальные объекты и информацию в реальное окружение пользователя, создавая уникальный опыт взаимодействия с миром. С каждым годом она становится все более популярной и широко применяемой как в развлекательных сферах, так и в индустрии, образовании, здравоохранении и многих других областях [1].

Эта технология открывает бескрайние возможности для улучшения обучения, упрощения повседневных задач, создания увлекательных игр или трансформации сценариев бизнес-процессов [2]. Однако, помимо потенциала, она представляет и ряд вызовов, связанных с безопасностью данных, эргономикой использования и влиянием на психологический комфорт пользователей.

В данной статье мы узнаем, что такое расширенная реальность, её применение в различных отраслях, преимущества и проблемы данной технологии, а также её будущие перспективы развития.

Что такое расширенная реальность?

Расширенная реальность — это динамичная и иммерсивная технология, которая объединяет физический и цифровой миры, предоставляя пользователям расширенные возможности. В ней сочетаются виртуальная реальность, дополненная реальность и смешанная реальность с их уникальными преимуществами [1, 3] (Рисунок 1).

Рисунок 1 – Схема моделей реальностей

Виртуальная реальность переносит пользователей в окружение, полностью созданное компьютером, создавая иммерсивную и зачастую интерактивную атмосферу. В этом случае пользователь должен использовать специальную гарнитуру для взаимодействия с цифровой средой. Виртуальная реальность создаёт новый искусственный мир, передаваемый человеку через его ощущения (зрение, слух, осязание и т.д.)

Дополненная реальность же лишь вносит отдельные искусственные элементы в восприятие мира реального. Известным примером дополненной реальности является игра «Pokémon Go», где при наведении камеры телефона пользователь видит местность, в которой находится, но с добавленными в неё «покемонами». В этой технологии обычно используются телефоны, планшеты или очки виртуальной реальности.

Смешанная реальность совмещает в себе элементы виртуальной и дополненной реальностей, позволяя взаимодействовать виртуальным и реальным объектам между собой. Самым свежим примером гарнитуры для смешанной реальности являются очки Apple Vision Pro. Apple позиционирует Vision Pro как «пространственный компьютер» (англ. spatial computer), объединяющий цифровые медиа с реальным окружением. При этом для взаимодействия с системой можно использовать физические элементы управления [2].

Применение расширенной реальности в различных отраслях

Применение расширенной реальности охватывает множество отраслей и областей, именно поэтому она является одним из наиболее захватывающих и перспективных направлений в современных технологиях.

1. Индустрия развлечений: одним из наиболее заметных примеров использования расширенной реальности является индустрия развлечений. Например, фильтры в приложениях, использующих камеру, которые добавляют на фото и видео в «Историях» различные визуальные и аудиоэффекты с использованием технологии дополненной реальности.
2. Образование: в образовании расширенная реальность может быть использована для создания интерактивных уроков, где учащиеся могут взаимодействовать с виртуальными моделями и симуляциями, углубляя своё понимание сложных концепций [4].
3. Медицина: в медицинской отрасли расширенная реальность применяется для тренировки хирургов, планирования операций и визуализации медицинских данных в реальном времени, что помогает повысить точность и эффективность лечения [3].
4. Розничная торговля: многие компании в области розничной торговли могут использовать расширенную реальность для улучшения опыта покупателей, позволяя им примерять виртуальную одежду или обувь перед покупкой.
5. Строительство и дизайн: в строительной отрасли расширенная реальность помогает архитекторам и дизайнерам визуализировать проекты в реальном масштабе, а также улучшить процессы проектирования и взаимодействия с заказчиками [5].
6. Туризм и культурное наследие: в туризме расширенная реальность может использоваться для создания интерактивных экскурсий, позволяющих туристам узнавать больше о местных достопримечательностях и истории.
7. Промышленность: в промышленности расширенная реальность применяется для обучения персонала, управления производственными процессами и создания инновационных решений для повышения производительности [4, 6].

8. Покупка и аренда жилья: с помощью расширенной реальности можно было бы просматривать варианты квартир и знакомиться с интерьером, не посещая саму жилплощадь [7].

Преимущества технологии

Как можно понять по информации, находящейся выше, появление расширенной реальности начало новую технологическую эру человечества. При правильном развитии технологии, расширенная реальность достаточно скоро сможет заменить человеку все гаджеты, совместив необходимые функции в одном устройстве. Она качественно улучшит жизнь людям, так как к её преимуществам относятся:

1. Улучшенное обучение: расширенная реальность может помочь студентам лучше понять сложные концепции, позволяя им взаимодействовать с виртуальными объектами и видеть, как они работают в реальном мире.
2. Улучшенная производительность: расширенная реальность может помочь рабочим более эффективно выполнять свои задачи, предоставляя им виртуальные инструкции и инструменты, которые они могут использовать для решения проблем.
3. Улучшенная навигация: расширенная реальность может помочь людям ориентироваться в незнакомых местах, предоставляя им виртуальные указатели и карты.
4. Улучшенная коммуникация: расширенная реальность может помочь людям общаться более эффективно, позволяя им видеть и взаимодействовать с виртуальными объектами, которые могут быть полезны для обсуждения.
5. Улучшенная безопасность: расширенная реальность может помочь людям работать в опасных условиях, предоставляя им виртуальные инструкции и инструменты, которые могут помочь им избежать ошибок.
6. Улучшенная доступность: расширенная реальность может помочь людям с ограниченными возможностями, предоставляя им виртуальные инструменты и инструкции, которые могут помочь им выполнять задачи, которые они иначе не смогли бы выполнить.
7. Улучшенные развлечения: расширенная реальность может подарить людям увлекательный опыт в развлекательно-игровой сфере, помогая отдохнуть и погрузиться в виртуальный мир [8, 9].

Проблемы расширенной реальности

Несмотря на имеющиеся преимущества, на сегодняшний день у расширенной реальности имеются важные проблемы, которые разработчикам придётся обязательно решить.

1. Стоимость: устройства расширенной реальности, такие как очки и гарнитуры, все еще довольно дороги. Это ограничивает их доступность для широкой аудитории.
2. Аккумуляторы: устройства расширенной реальности требуют большого количества энергии для работы, что приводит к быстрому разряду батареи. Это может быть особенно проблематично для пользователей, которые хотят использовать расширенную реальность в течение длительного времени.
3. Здоровье и безопасность: некоторые исследования показывают, что длительное использование устройств расширенной реальности может вызвать проблемы со зрением и головные боли. Кроме того, устройства расширенной реальности могут представлять опасность для пользователей, если они не обращают внимания на окружающую среду.

4. Отслеживание и позиционирование: устройства расширенной реальности должны точно отслеживать и позиционировать объекты в реальном мире, чтобы создать точное и реалистичное изображение. Это может быть сложно в некоторых условиях, таких как яркий свет или быстрые движения.

5. Приватность и конфиденциальность: устройства расширенной реальности могут собирать большое количество данных о пользователях, включая их местоположение и действия. Это может вызвать проблемы с приватностью и конфиденциальностью.

6. Ограниченная функциональность: хотя устройства расширенной реальности имеют большой потенциал, они все еще ограничены в том, что они могут делать. Например, они не могут полностью заменить реальный мир или создать полностью реалистичные виртуальные объекты.

7. Ограниченная доступность контента: хотя существует множество приложений и игр для расширенной реальности, доступность контента все еще ограничена. Это может быть особенно проблематично для пользователей, которые хотят использовать дополненной реальности для работы или образования [10].

Перспективы развития расширенной реальности в будущем

На данный момент расширенная реальность является одним из наиболее перспективных направлений среди современных технологий, поэтому стоит ожидать внедрения её во все сферы нашей жизни и постоянного улучшения данной области. В будущем будут появляться всё новые способы использования расширенной реальности в разных формах деятельности. Важно, чтобы со временем данная технология стала доступной для обычного человека, для чего нужно модернизировать имеющееся оборудование и гарнитуры.

Ожидается, что рынок расширенной реальности будет расти в среднем на 34.94% со 105.58 млрд долларов США в 2023 году до 472 млрд долларов США к 2028 году. Ключевыми факторами роста этого рынка являются растущее внедрение технологий виртуальной и дополненной реальностей, а также по мере роста использования подключенных устройств и смартфонов все большим количеством игроков рынка [5].

Выводы

Расширенная реальность — это технология, которая позволяет нам видеть и взаимодействовать с цифровыми объектами в нашем реальном мире. Она имеет множество применений, от игр и развлечений до медицины и образования.

Расширенная реальность имеет огромный потенциал для улучшения нашей жизни. Она может помочь нам лучше понимать окружающий мир, улучшить наши навыки и знания, а также сделать нашу жизнь более интересной и увлекательной.

Расширенная реальность увеличивает эффективность продаж во многих отраслях, включая, в первую очередь, розничную торговлю и развлечения. Конечно, разработчикам предстоит совершить много открытий и преодолеть много препятствий для создания по-настоящему полезных и впечатляющих решений. Но похоже, что уже сегодня мы близки к эпохе, когда реальный опыт будет сложно отличить от виртуального.

Список литературы

1. Расширенная реальность: руководство по XR // Unity URL: Подробный обзор расширенной реальности (XR), курсы и многое другое | Unity (Дата обращения: 20.03.2024).
2. Википедия, Apple Vision Pro URL: Apple Vision Pro — Википедия (wikipedia.org) (Дата обращения: 20.03.2024).
3. XRinSurgery // Experimental Surgery Berlin URL: FutureOR | XR in Surgery (experimental-surgery.de) (Дата обращения: 20.03.2024).
4. Что такое расширенная реальность? // Setphone URL: Что такое расширенная реальность? (setphone.ru) (Дата обращения: 20.03.2024).
5. Расширенная реальность: ключевые детали, которые вам нужно знать // TargetTrend URL: Расширенная реальность: ключевые детали, которые вам нужно знать - TargetTrend (Дата обращения: 20.03.2024).
6. Мошуров В.М., Сафонова Т.В., Вершинин А.К., Ясников А.И., Логинов И.С. Область применения агентных платформ ФГБОУ ВО РГГМУ Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 46-52.
7. Полтавцева Е.А., Сафонова Т.В. Облачные решения для развития производства Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 80-86.
8. Булгакова А.В., Сафонова Т.В., Кирспуу К.А. Применение облачных решений на предприятии Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 71-76.
9. Ясников А.И., Сафонова Т.В., Русскин В.Д., Логинов И.С., Мошуров В.М. Использование технологий виртуальной реальности в обучении Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 60-69.
10. Анализ размера и доли рынка расширенной реальности - тенденции роста и прогнозы (2023 - 2028 гг.) Электронный ресурс – Режим доступа: https://www.mordorintelligence.com/ru/industry-reports/extended-reality-xr-market (Date of access: 03/27/24).

References

1. Augmented Reality: XR Guide // Unity URL: Detailed Overview of Augmented Reality (XR), courses and more | Unity(Accessed 03/20/2024).
2. Wikipedia, Apple Vision Pro URL: Apple Vision Wikipedia (wikipedia.org) (Date of application: 03/20/2024).
3. XRinSurgery // Experimental Surgery Berlin URL: FutureOR | XR in Surgery (experimental-surgery.de) (Date of access: 03/20/2024).
4. What is augmented reality? // Setphone URL: What is Augmented Reality? (setphone.ru) (Date of application: 03/20/2024).
5. Augmented reality: key details that you need to know // TargetTrend URL: Augmented reality: key details that you need to know - TargetTrend (Date of access: 03/20/2024).
6. Moshurov V.M., Safonova T.V., Vershinin A.K., Yasnikov A.I., Loginov I.S. Scope of application of agent-based Information Technologies and Systems: management, Economics, transport, law. 2023. No. 1 (45). pp. 46-52.

7. Poltavtseva E.A., Safonova T.V. Cloud solutions for the development of production Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 80-86.
8. Bulgakova A.V., Safonova T.V., Kirspuu K.A. Application of cloud solutions in the enterprise Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 71-76.
9. Yasnikov A.I., Safonova T.V., Ruskin V.D., Loginov I.S., Moshurov V.M. The use of virtual reality technologies in teaching Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 60-69.
10. Analysis of the size and share of the augmented reality market - growth trends and forecasts (2023-2028) Electronic resource – Access mode: https://www.mordorintelligence.com/ru/industry-reports/extended-reality-xr-market (Date of access: 03/27/24).

Перевертун Д.Р. Роль искусственного интеллекта в информационной безопасности // Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 92–97

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.8

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

В статье рассматривается роль искусственного интеллекта (ИИ) в сфере информационной безопасности, охватывая его использование для обнаружения и предотвращения кибератак, анализа и классификации вредоносного программного обеспечения, а также прогнозирования будущих угроз. Освещаются преимущества, возможности и перспективы применения ИИ, включая повышение эффективности защиты информационных систем и адаптацию к эволюционирующему ландшафту угроз. Однако статья также подчеркивает существующие риски и проблемы, связанные с приватностью, этическими вопросами и потенциалом злоупотреблений.

Ключевые слова: Искусственный интеллект, информационная безопасность, кибератаки, вредоносное ПО, прогнозирование угроз, машинное обучение, управление рисками, этические вопросы, приватность данных, обучение специалистов, международное сотрудничество.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article examines the role of artificial intelligence (AI) in the field of information security, covering its use to detect and prevent cyber attacks, analyze and classify malicious software, as well as predict future threats. The advantages, opportunities and prospects of AI application are highlighted, including increasing the effectiveness of information system protection and adaptation to the evolving threat landscape. However, the article also highlights the existing risks and challenges related to privacy, ethical issues and the potential for abuse.

Keywords: Artificial intelligence, information security, cyber attacks, malware, threat forecasting, machine learning, risk management, ethical issues, data privacy, training of specialists, international cooperation.

Искусственный интеллект может быть использован в информационной безопасности для решения различных задач, включая обнаружение угроз, анализ и классификацию вредоносного ПО, а также прогнозирование и предотвращение кибератак. Системы на основе ИИ способны анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые угрозы, что значительно повышает эффективность защиты информационных систем.

Одним из основных направлений применения ИИ в информационной безопасности является обнаружение угроз. Алгоритмы машинного обучения могут обучаться на исторических данных о кибератаках, что позволяет им эффективно распознавать потенциально опасные действия в сети. Такие системы способны не только обнаруживать известные виды атак, но и предсказывать новые, еще неизвестные угрозы, адаптируясь к постоянно меняющемуся ландшафту кибербезопасности.

Одним из наиболее перспективных направлений использования искусственного интеллекта в области информационной безопасности является обнаружение и предотвращение угроз. Искусственный интеллект вносит значительный вклад в повышение эффективности и актуальности мер по обеспечению кибербезопасности, адаптируясь к постоянно меняющемуся ландшафту угроз.

Системы на основе ИИ способны анализировать огромные объемы данных в реальном времени, что включает в себя трафик сети, журналы операций, а также разнообразные внешние источники информации. Этот анализ позволяет выявлять аномалии и нестандартное поведение, которые могут указывать на попытку несанкционированного доступа, распространение вредоносного ПО или другие виды кибератак.[5] Основываясь на обнаруженных данных, ИИ может с высокой степенью точности определить потенциальную угрозу, даже если она маскируется под легитимные процессы или использует ранее неизвестные методы атаки.

Благодаря способности к обучению, системы ИИ с течением времени становятся только эффективнее в определении угроз, учитывая новые вирусные сигнатуры, тактики, техники и процедуры, используемые киберпреступниками. Это позволяет не только реагировать на текущие угрозы, но и прогнозировать потенциальные атаки, адаптируя защитные механизмы в соответствии с изменениями в поведении атакующих.

Таким образом, внедрение искусственного интеллекта в системы обнаружения и предотвращения угроз позволяет значительно повысить уровень защищенности информационных систем, сократить время на обнаружение и нейтрализацию атак, а также оптимизировать процессы принятия решений в области кибербезопасности.[3] Это становится особенно важным в условиях постоянно растущего количества угроз и их сложности, где традиционные методы защиты уже не способны обеспечить должный уровень безопасности.

Системы ИИ также находят применение в анализе и классификации вредоносного программного обеспечения. Используя методы глубокого обучения, они могут анализировать поведение ПО, выявлять скрытые вредоносные функции и даже предсказывать потенциальное поведение нового ПО на основе сходства с уже известными вирусами и троянами.

Применение искусственного интеллекта в анализе и классификации вредоносного программного обеспечения является одним из наиболее важных направлений в области кибербезопасности. Развитие технологий ИИ позволило создать системы, способные самостоятельно обучаться на основе анализа больших объемов данных, что значительно увеличивает их эффективность в распознавании и классификации вредоносного ПО.

Данные системы используют различные методы машинного обучения, включая обучение с учителем, без учителя и обучение с подкреплением, для анализа поведенческих паттернов, сигнатур и других характеристик вредоносных программ. Это позволяет не только определять уже известное вредоносное ПО на основе существующих баз данных сигнатур, но и выявлять новые, ранее неизвестные угрозы.[1] Анализ происходит путем сравнения с

обширным набором признаков, характерных для вредоносного кода, что включает в себя анализ поведения, изменения в системных файлах и регистрах, сетевую активность и другие факторы.

Благодаря возможности анализировать и обрабатывать огромные объемы данных в кратчайшие сроки, ИИ значительно ускоряет процесс идентификации вредоносного ПО. Это особенно важно в условиях современного киберпространства, где каждую минуту создаются новые варианты вредоносных программ.[7] Кроме того, ИИ способен обучаться на основе анализа поведения вредоносного ПО в динамике, что позволяет ему предсказывать потенциальные угрозы на основе обнаруженных поведенческих моделей и принимать меры по их нейтрализации еще до того, как они успеют нанести ущерб.

Внедрение ИИ в процессы анализа и классификации вредоносного ПО также способствует повышению точности определения угроз, снижая количество ложноположительных и ложноотрицательных срабатываний, которые могут привести к ненужной тревоге или, наоборот, пропуску реальной угрозы. Это достигается за счет того, что ИИ способен адаптироваться к изменениям в методах атак и поведении вредоносного ПО, постоянно обновляя свои алгоритмы на основе получаемой информации.

Применение ИИ не ограничивается обнаружением и анализом угроз; оно также включает в себя прогнозирование кибератак. Системы могут анализировать тенденции и модели поведения в сети, выявляя потенциальные уязвимости и прогнозируя вероятные направления атак. Это позволяет предпринимать профилактические меры до того, как угроза реализуется.

Прогнозирование кибератак с использованием искусственного интеллекта является одной из наиболее инновационных и перспективных областей в сфере информационной безопасности. Эта технология предоставляет возможность не только реагировать на уже произошедшие или текущие атаки, но и предвидеть потенциальные угрозы до того, как они могут быть реализованы.[2] Основываясь на сложных алгоритмах машинного обучения и анализе больших данных, системы на основе искусственного интеллекта способны выявлять закономерности и взаимосвязи в данных о кибербезопасности, которые могут указывать на предвестники будущих атак.

Эти системы анализируют широкий спектр данных, включая, но не ограничиваясь, журналами событий безопасности, сетевым трафиком, тенденциями в интернете, обсуждениями на форумах хакеров, утечками данных и другими источниками информации, которые могут предоставить индикаторы потенциальной угрозы. Путем обработки и анализа этих данных, ИИ может выявить неочевидные связи и закономерности, которые могут не быть очевидны для человека или традиционных систем безопасности.

Прогнозирование кибератак с помощью ИИ позволяет не только предсказывать специфические атаки, но и определять вероятные цели атак и методы, которые могут быть использованы злоумышленниками. Это дает организациям возможность заблаговременно укрепить защиту наиболее уязвимых точек, разработать и внедрить профилактические меры и стратегии реагирования на инциденты, а также провести обучение персонала для повышения уровня осведомленности о потенциальных угрозах.

Однако, несмотря на значительный потенциал, прогнозирование кибератак с использованием искусственного интеллекта сталкивается с рядом вызовов. Среди них – сложность обработки и интерпретации огромного количества данных, необходимость в постоянном обновлении информационной базы для адаптации к постоянно меняющемуся

ландшафту угроз, а также потенциальные риски, связанные с ложноположительными срабатываниями, которые могут привести к неоправданным затратам ресурсов на неверные угрозы.

Несмотря на эти трудности, прогнозирование кибератак с использованием искусственного интеллекта продолжает развиваться, предлагая новые возможности для повышения эффективности систем кибербезопасности.[6] Совершенствование технологий ИИ и улучшение методик анализа данных обещают значительное увеличение точности и оперативности прогнозирования угроз, что позволит еще более эффективно противостоя

Внедрение искусственного интеллекта (ИИ) в область информационной безопасности, несмотря на свои очевидные преимущества, также сопровождается рядом возможных рисков и проблем. Эти вызовы охватывают технические, этические и операционные аспекты, требующие тщательного анализа и управления.

Одной из ключевых проблем является зависимость систем безопасности на основе ИИ от качества и объема обучающих данных. Для эффективного обучения модели ИИ требуют доступ к большим и разнообразным наборам данных, которые должны быть актуальными и репрезентативными. Однако, сбор таких данных может столкнуться с проблемами конфиденциальности и защиты персональных данных, а также с риском включения в обучающий набор предвзятых или некорректных данных, что может привести к ошибочным выводам и действиям со стороны ИИ.

Другой серьезной проблемой является угроза создания и использования вредоносного ИИ. Такие системы могут быть разработаны для проведения кибератак, например, для автоматизации фишинговых атак, обхода систем обнаружения вторжений или даже для разработки новых видов вредоносного ПО, способного эффективнее скрываться от традиционных средств защиты.

Кроме того, использование ИИ в информационной безопасности порождает ряд этических вопросов, связанных с прозрачностью и объяснимостью принимаемых системой решений. Важность этих вопросов возрастает в тех случаях, когда неправильные решения могут привести к серьезным последствиям, таким как неверное блокирование законных операций или нарушение конфиденциальности пользовательских данных.

Техническая сложность систем на основе ИИ также поднимает вопросы об их уязвимости для кибератак. Модели ИИ могут стать целью атак, направленных на искажение их работы путем подачи специально подготовленных данных (атаки с использованием "ядовитых" данных), что может привести к непредсказуемым и нежелательным последствиям.[4]

Наконец, необходимо учитывать и проблему недостаточной квалификации персонала. Эффективное использование ИИ в информационной безопасности требует специалистов, обладающих не только знаниями в области кибербезопасности, но и пониманием принципов работы и возможностей искусственного интеллекта. Недостаток таких специалистов может ограничить способность организаций полноценно использовать потенциал ИИ для укрепления своих систем безопасности.

Таким образом, несмотря на значительный потенциал искусственного интеллекта в усилении информационной безопасности, необходимо тщательно управлять связанными с его использованием рисками и проблемами, разрабатывая стратегии и меры, направленные на минимизацию возможных негативных последствий. Важными аспектами такого управления

являются разработка стандартов и процедур для обеспечения качества и безопасности данных, используемых для обучения ИИ, установление этических принципов использования искусственного интеллекта в целях информационной безопасности, а также внедрение процедур регулярной оценки и корректировки алгоритмов ИИ для предотвращения их злоупотребления или ошибочного функционирования.

В заключение, роль искусственного интеллекта (ИИ) в информационной безопасности продолжает набирать обороты, предлагая передовые решения для обнаружения угроз, предотвращения атак, анализа и классификации вредоносного ПО, а также прогнозирования кибератак. Эти технологии обещают значительное улучшение способности организаций защищать свои информационные активы в условиях постоянно развивающегося и усложняющегося ландшафта киберугроз.

Однако внедрение ИИ в системы кибербезопасности также сопряжено с рядом вызовов и рисков, включая вопросы этики, приватности, зависимости от качества данных и угрозы использования вредоносного ИИ. Эффективное управление этими рисками требует комплексного подхода, который включает в себя разработку нормативных стандартов, обеспечение прозрачности и объяснимости решений ИИ, а также постоянное обучение и повышение квалификации специалистов.

По мере развития технологий искусственного интеллекта и углубления понимания их потенциала и ограничений, можно ожидать, что их роль в области кибербезопасности будет только усиливаться. Инвестиции в исследования и разработку, а также в создание международных рамок сотрудничества будут ключевыми факторами в реализации полного потенциала ИИ для защиты информационного пространства от киберугроз.

Таким образом, будущее информационной безопасности неразрывно связано с прогрессом в области искусственного интеллекта. Успех в этой области потребует не только технологических инноваций, но и продуманного подхода к решению этических, правовых и образовательных вопросов, обеспечивающих безопасное, ответственное и эффективное использование ИИ.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.

6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.

Нижлукченко И.Д. Фишинговые атаки и как их распознать: анализ наиболее распространенных методик фишинга и советы по их идентификации и предотвращению // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 98–103

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ФИШИНГОВЫЕ АТАКИ И КАК ИХ РАСПОЗНАТЬ: АНАЛИЗ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ МЕТОДИК ФИШИНГА И СОВЕТЫ ПО ИХ ИДЕНТИФИКАЦИИ И ПРЕДОТВРАЩЕНИЮ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

Эта статья представляет собой всесторонний анализ фишинговых атак, их специфики, наиболее распространенных методик, а также стратегий для их идентификации и предотвращения. Освещая тему с различных аспектов, статья детально рассматривает механизмы, с помощью которых злоумышленники осуществляют атаки, предоставляя читателю глубокое понимание того, как фишинговые сообщения создаются и распространяются через электронную почту, социальные сети, SMS и другие цифровые каналы. Помимо этого, в статье предлагаются практические советы по обеспечению кибербезопасности, включая использование технических средств защиты и образовательных программ для снижения риска фишинговых атак. Анализируется важность анализа и отчетности в борьбе против киберпреступности, подчеркивая значимость совместных усилий в обмене информацией и разработке стратегий защиты.

Ключевые слова: Фишинг, кибербезопасность, идентификация фишинга, предотвращение фишинга, методики фишинга, анализ фишинговых атак, защита от фишинга, образование в области кибербезопасности.

PHISHING ATTACKS AND HOW TO RECOGNIZE THEM: AN ANALYSIS OF THE MOST COMMON PHISHING TECHNIQUES AND TIPS FOR IDENTIFYING AND PREVENTING THEM

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

This article provides a comprehensive analysis of phishing attacks, their specifics, the most common techniques, as well as strategies for their identification and prevention. Covering the topic from various aspects, the article examines in detail the mechanisms by which attackers carry out attacks, providing the reader with a deep understanding of how phishing messages are created and distributed through email, social networks, SMS and other digital channels. In addition, the article offers practical tips on ensuring cybersecurity, including the use of technical means of protection and educational programs to reduce the risk of phishing attacks. The importance of analysis and reporting in the fight against cybercrime is analyzed, emphasizing the importance of joint efforts in the exchange of information and the development of protection strategies.

Keywords: Phishing, cybersecurity, phishing identification, phishing prevention, phishing techniques, phishing attack analysis, phishing protection, cybersecurity education.

В последние десятилетия интернет стал неотъемлемой частью нашей повседневной жизни. Этот цифровой мир предоставил невероятные возможности для обучения, ведения бизнеса и общения. Однако, вместе с прогрессом пришли и новые угрозы, одной из которых являются фишинговые атаки. Фишинг — это тип кибератаки, цель которой заключается в том, чтобы обманом заставить жертву раскрыть конфиденциальную информацию, такую как пароли, данные кредитных карт и банковские сведения. Эта статья направлена на анализ наиболее распространенных методик фишинга, предоставление советов по их идентификации и предотвращению.

Фишинговые атаки часто маскируются под легитимные запросы от известных компаний или социальных сетей. Атакующие используют различные платформы: электронную почту, социальные сети, SMS и веб-сайты. Сообщения могут содержать прямые призывы к действию, такие как подтверждение учетной записи или изменение пароля, и часто сопровождаются ссылками на поддельные веб-сайты, визуально неотличимые от настоящих.

Фишинговые атаки имеют свою уникальную специфику, которая выделяет их среди других видов киберугроз. Эти атаки основаны на манипуляции и обмане, где злоумышленники стараются выдать себя за доверенные лица или организации. Часто фишинговые сообщения выглядят как официальные запросы от известных компаний, банков или социальных сетей, и могут призывать жертву к срочным действиям — например, подтвердить учетную запись или обновить пароль. Эти сообщения могут приходить через различные каналы коммуникации, включая электронную почту, мессенджеры, социальные сети и даже SMS.

Одним из характерных признаков фишинга является использование поддельных веб-сайтов, которые внешне почти не отличаются от настоящих.[3] Злоумышленники тщательно копируют дизайн и структуру реальных сайтов, чтобы убедить пользователя в подлинности своего запроса. При этом, даже минимальное несоответствие в адресе сайта или в его визуальном оформлении может выдать подделку. Особенно это касается случаев, когда для перехода на сайт используются ссылки из сообщений: они могут вести на вредоносные страницы, где пользователь, не подозревая обмана, вводит свои конфиденциальные данные.

Эти атаки опираются на элемент неожиданности и психологическое давление. Зачастую жертвам предлагается немедленно предпринять какие-то действия, чтобы избежать негативных последствий, таких как блокировка аккаунта или потеря средств. Этот метод спешки создает условия, при которых человек менее склонен задумываться о подлинности запроса и больше подвержен риску совершить ошибку. Именно эта специфика делает фишинговые атаки особенно опасными, поскольку они направлены на эксплуатацию человеческого фактора, а не технических уязвимостей системы.

Методики фишинга разнообразны и постоянно эволюционируют, поскольку злоумышленники ищут новые способы обмана пользователей и обхода систем безопасности. В основе фишинга лежит психологический маневр, направленный на вызов доверия или страха, чтобы мотивировать жертву к действию, чаще всего к разглашению конфиденциальной информации. В этом контексте фишинг адаптируется к различным сценариям использования и технологическим платформам, чтобы максимально увеличить свою эффективность.

Одним из основных методов является спир-фишинг, который отличается высокой степенью персонализации. Злоумышленники собирают информацию о своих целях, используя

открытые источники или предыдущие утечки данных, чтобы создать сообщения, кажущиеся максимально достоверными. Эти сообщения могут имитировать переписку от коллег, друзей или руководителей, часто ссылаясь на конкретные детали, знакомые жертве, что делает атаку особенно убедительной.

Вайлинг углубляет концепцию спир-фишинга, нацеливаясь на верхушку иерархической лестницы — высокопоставленных руководителей организаций. В этих случаях сообщения могут содержать запросы на перевод средств или предоставление конфиденциальной корпоративной информации, маскируясь под срочные деловые потребности.

Фарминг, в отличие от других методов, фокусируется на техническом манипулировании, направленном на перенаправление пользователей с легитимных сайтов на поддельные, часто с помощью заражения DNS-серверов или внедрения вредоносного ПО. Этот метод позволяет атакующим перехватывать данные пользователя незаметно для него.

Смишинг и вишинг применяют традиционные каналы связи, такие как SMS и телефонные звонки, для доставки фишинговых сообщений. Эти атаки используют схемы, в которых злоумышленники выдают себя за представителей банков или других уважаемых организаций, убеждая жертву предоставить личную информацию или выполнить финансовые операции под предлогом проверки счета или обновления безопасности.

В целом, разнообразие методик фишинга отражает адаптивность и изобретательность злоумышленников в их стремлении обмануть пользователей. Эффективная защита требует постоянного осведомления о новых методах атак и культуры безопасного поведения в интернете.

Идентификация и предотвращение фишинговых атак требуют комплексного подхода, который включает в себя образование пользователей, использование технических средств безопасности и внедрение строгих процедур обработки информации. Одной из ключевых стратегий является развитие критического мышления и бдительности при работе с электронной почтой и другими цифровыми каналами.[5] Пользователи должны научиться распознавать потенциальные признаки фишинговых сообщений, такие как несоответствие адреса отправителя, наличие орфографических и грамматических ошибок, странное форматирование и необычное использование языка, а также подозрительные призывы к действию.

Обучение и повышение осведомленности среди сотрудников и пользователей играет важную роль в предотвращении фишинга. Регулярные тренинги и симуляции фишинговых атак могут помочь людям лучше понять, как выглядят фишинговые атаки в реальности, и как на них правильно реагировать. Кроме того, важно подчеркнуть необходимость осторожного отношения к личной и корпоративной информации, учить не раскрывать ее без достаточной проверки легитимности запроса.

На техническом уровне, использование современных инструментов безопасности, таких как антивирусное и антифишинговое программное обеспечение, может значительно уменьшить риск успешной фишинговой атаки.[2] Эти инструменты могут автоматически отфильтровывать подозрительные письма, предупреждать пользователей о потенциально опасных сайтах и блокировать доступ к известным вредоносным ресурсам.

Двухфакторная аутентификация представляет собой еще один эффективный способ защиты от последствий фишинговых атак, поскольку даже в случае компрометации логина и

пароля злоумышленникам будет значительно сложнее получить доступ к защищаемым ресурсам без второго фактора аутентификации.

Важной частью стратегии предотвращения фишинга является также разработка и внедрение четких процедур обработки запросов на доступ к информации или выполнение финансовых операций. Это включает в себя требования к двойной проверке и подтверждению таких запросов через альтернативные каналы связи, что значительно усложняет задачу для атакующих.

В совокупности, эти меры формируют многоуровневую систему защиты, которая помогает снизить риск успешных фишинговых атак и минимизировать их потенциальный ущерб.

В борьбе с фишинговыми атаками принятие эффективных мер предосторожности является ключевым элементом защиты как индивидуальных пользователей, так и организаций в целом. Важным шагом в этом направлении является укрепление системы аутентификации пользователей. Внедрение двухфакторной аутентификации значительно увеличивает безопасность, поскольку даже в случае, если злоумышленники сумеют узнать пароль пользователя, дополнительный уровень проверки может предотвратить несанкционированный доступ к учетной записи.

Помимо технических средств, большое значение имеет повышение осведомленности и образовательный аспект. Регулярное обучение сотрудников и пользователей, проведение тренингов по кибербезопасности и симуляции фишинговых атак помогают развивать критическое мышление и учат распознавать потенциальные угрозы.[4] Ведь осознанное отношение к безопасности в интернете и умение идентифицировать подозрительные сообщения и веб-страницы являются мощным инструментом противодействия фишингу.

Кроме того, регулярное резервное копирование данных обеспечивает дополнительный уровень защиты. В случае успешной фишинговой атаки, направленной на кражу или шифрование данных, наличие актуальных копий позволяет быстро восстановить информацию и минимизировать потери.

Использование специализированного программного обеспечения для защиты от фишинга также играет важную роль в обеспечении кибербезопасности. Антивирусные и антифишинговые решения могут автоматически блокировать доступ к известным вредоносным сайтам, анализировать входящие сообщения на предмет подозрительного содержимого и предупреждать пользователей о потенциальных угрозах.

В совокупности, эти меры предосторожности создают многоуровневую защиту, которая охватывает как технические аспекты безопасности, так и человеческий фактор. Внедрение комплексного подхода к кибербезопасности, включающего как передовые технологии, так и постоянное обучение и повышение осведомленности, является наиболее эффективной стратегией противодействия фишинговым атакам.Анализ и отчетность

Анализ и отчетность о фишинговых атаках играют ключевую роль в цикле улучшения кибербезопасности организации. Этот процесс начинается с момента обнаружения подозрительной активности или атаки и включает в себя сбор, анализ и документирование всех доступных данных о произошедшем инциденте.[1] Основная цель здесь — не только фиксация ущерба или потенциального ущерба от атаки, но и извлечение уроков, которые помогут предотвратить подобные инциденты в будущем.

Как только атака идентифицирована, специалисты по кибербезопасности приступают к детальному анализу методов и инструментов, использованных злоумышленниками. Это включает в себя изучение векторов атаки, таких как способы доставки фишинговых сообщений, использование вредоносных ссылок или вложений, а также методы маскировки и обхода защитных механизмов. Анализируя эти данные, команда безопасности может выявить уязвимые места в текущей системе защиты и разработать рекомендации по их устранению.

После сбора и анализа информации следует этап отчетности. Составление подробных отчетов о фишинговых атаках и их последствиях позволяет руководству организации и специалистам по безопасности оценить масштаб проблемы и эффективность внедренных мер безопасности. Отчеты могут включать в себя описание использованных атакующими методик, идентифицированные уязвимости, оценку ущерба, а также предложения по улучшению системы кибербезопасности.

Важным аспектом анализа и отчетности является обмен информацией не только внутри организации, но и с внешними структурами, такими как правоохранительные органы, другие компании и специализированные сообщества по кибербезопасности. Это позволяет расширить базу данных о фишинговых атаках, способствовать кооперации в борьбе с киберпреступностью и повысить общий уровень защищенности в цифровом пространстве.

Таким образом, анализ и отчетность не только фиксируют опыт борьбы с фишингом, но и способствуют накоплению знаний, которые могут быть использованы для предотвращения будущих атак, повышения устойчивости инфраструктуры и формирования культуры кибербезопасности среди пользователей и сотрудников

Фишинг остается одной из наиболее распространенных и эффективных форм кибератак, наносящих значительный ущерб как отдельным лицам, так и организациям. Распознавание признаков фишинга, применение мер предосторожности и постоянное обучение являются ключевыми элементами защиты от этих угроз. В то время как технологии безопасности продолжают развиваться, осознанное отношение к кибербезопасности и проактивные действия пользователей играют решающую роль в обеспечении безопасности в цифровом мире.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского

государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.

5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Перевертун Д.Р. Угрозы информационной безопасности: всесторонний анализ// Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 104–108

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВСЕСТОРОННИЙ АНАЛИЗ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Статья представляет всесторонний анализ угроз информационной безопасности, рассматривая их многообразие и динамическое развитие в современном цифровом мире. Основное внимание уделено классификации угроз, включая вредоносное ПО, атаки на уязвимости, социальную инженерию, внутренние угрозы и кибершпионаж. Помимо этого, рассмотрены методы предотвращения и противодействия угрозам, охватывающие как технические, так и организационные аспекты, включая использование искусственного интеллекта, обучение персонала, и разработку комплексных политик безопасности. В заключение представлены будущие тенденции в области информационной безопасности, подчеркивая роль инноваций и международного сотрудничества в адаптации к эволюционирующим угрозам.

Ключевые слова: Информационная безопасность, киберугрозы, вредоносное ПО, атаки на уязвимости, социальная инженерия, внутренние угрозы, кибершпионаж, предотвращение угроз, искусственный интеллект, международное сотрудничество, будущие тенденции.

THREATS TO INFORMATION SECURITY: A COMPREHENSIVE ANALYSIS

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article presents a comprehensive analysis of information security threats, considering their diversity and dynamic development in the modern digital world. The main focus is on the classification of threats, including malware, vulnerability attacks, social engineering, internal threats and cyber espionage. In addition, methods of preventing and countering threats are considered, covering both technical and organizational aspects, including the use of artificial intelligence, personnel training, and the development of comprehensive security policies. In conclusion, future trends in the field of information security are presented, emphasizing the role of innovation and international cooperation in adapting to evolving threats.

Keywords: Information security, cyber threats, malware, vulnerability attacks, social engineering, internal threats, cyber espionage, threat prevention, artificial intelligence, international cooperation, future trends.

Угрозы информационной безопасности можно классифицировать на несколько основных категорий: вредоносные программы, атаки на уязвимости, социальная инженерия, внутренние угрозы и кибершпионаж. Вредоносные программы включают в себя вирусы, трояны, шпионское и рекламное ПО, которые могут привести к утечке конфиденциальной

информации, потере данных или даже полному контролю над системой. Атаки на уязвимости эксплуатируют пробелы в безопасности программного обеспечения и операционных систем. Социальная инженерия направлена на манипулирование людьми для получения доступа к закрытой информации. Внутренние угрозы исходят от сотрудников организации, которые могут нанести ущерб, имея легитимный доступ к ресурсам. Кибершпионаж охватывает деятельность, направленную на незаконное получение секретной информации с целью получения преимущества.

В контексте информационной безопасности современный цифровой ландшафт представляет собой многоуровневую систему, в которой различные угрозы переплетаются и взаимодействуют друг с другом, создавая сложную и постоянно меняющуюся картину рисков. Эти угрозы происходят не изолированно, а формируются в рамках широкого спектра действий и акторов, каждый из которых имеет свои мотивы, цели и методы.

На первом уровне находятся вредоносные программы, которые, будучи разработаны для выполнения нежелательных и часто вредоносных действий, способны внедряться в системы, оставаясь незамеченными. Их цели могут варьироваться от простого раздражения пользователей до кражи конфиденциальных данных и дестабилизации критически важной инфраструктуры.

Далее, атаки на уязвимости представляют собой сознательное использование слабых мест в программном обеспечении и системах для проникновения или нарушения их нормального функционирования. Эти уязвимости могут быть как вновь обнаруженными, так и уже известными, но не устраненными из-за различных причин, включая недостаток ресурсов или знаний.

Социальная инженерия выступает как метод манипулирования людьми для обхода традиционных мер безопасности. Эта тактика основана на использовании психологических приемов для введения в заблуждение и получения несанкционированного доступа к информации или системам.

Внутренние угрозы, исходящие от самих сотрудников организации, могут быть как непреднамеренными, так и умышленными. Непреднамеренные угрозы часто связаны с недостаточным пониманием или игнорированием политик безопасности, в то время как умышленные действия могут включать в себя кражу данных, саботаж или другие вредоносные действия.[4]

Наконец, кибершпионаж, используемый государственными и негосударственными акторами для получения конфиденциальной информации без ведома и согласия владельца, демонстрирует сложность и масштаб угроз в современном мире. Эта деятельность направлена на получение стратегического преимущества в политических, экономических или военных сферах.

Эти угрозы не являются статичными; они развиваются вместе с технологическим прогрессом, становясь всё более изощренными и трудноуловимыми. Борьба с ними требует комплексного подхода, включающего технологические, организационные и образовательные меры, а также постоянное сотрудничество между организациями и государствами.

Для обеспечения информационной безопасности используются комплексные меры, включающие как технические, так и организационные аспекты. К техническим мерам относятся использование антивирусного и антиспамного ПО, файерволов, систем обнаружения и предотвращения вторжений, а также регулярное обновление ПО для

устранения уязвимостей.[2] Организанизационные меры включают разработку и внедрение политик информационной безопасности, обучение персонала принципам безопасного обращения с информацией, регулярные аудиты и проверки безопасности для выявления и устранения потенциальных уязвимостей. Важным элементом является также создание системы реагирования на инциденты, что позволяет оперативно принимать меры при обнаружении угрозы.

В области информационной безопасности методы предотвращения угроз объединяются в комплексный подход, включающий в себя разнообразные стратегии и технологии, направленные на защиту информационных систем от широкого спектра угроз. Этот подход требует интеграции технических средств, организационных мер и образовательных программ для создания эффективной обороны против внешних и внутренних атак.

На техническом уровне внедрение современных антивирусных программ и межсетевых экранов служит первой линией защиты, блокируя вредоносное ПО и нежелательный сетевой трафик. Дополнительно, системы обнаружения и предотвращения вторжений анализируют сетевой трафик в реальном времени, выявляя и нейтрализуя потенциальные угрозы.[7] Регулярное обновление программного обеспечения и операционных систем устраняет известные уязвимости, снижая риск успешных атак.

Организационные меры предполагают разработку и внедрение политик информационной безопасности, которые определяют стандарты поведения и процедуры для защиты информационных ресурсов. Эти политики охватывают такие аспекты, как управление доступом, шифрование данных, физическая безопасность и реагирование на инциденты. Важной частью организационных мер является также разработка плана реагирования на инциденты, который обеспечивает быструю и организованную реакцию на угрозы и атаки, с целью минимизации ущерба и восстановления нормальной работы систем.

Образовательные программы играют ключевую роль в повышении осведомленности сотрудников об угрозах информационной безопасности и методах их предотвращения. Регулярное обучение и тренировки помогают сотрудникам осознать значение безопасного поведения в интернете, правила создания надежных паролей, опасности социальной инженерии и другие аспекты, критически важные для обеспечения безопасности организации.[5]

Таким образом, методы предотвращения угроз в области информационной безопасности представляют собой сложную и многоуровневую систему, требующую не только применения передовых технологий, но и активного участия всех сотрудников организации, а также постоянного обновления знаний и навыков в соответствии с меняющейся средой угроз.

С учетом постоянного развития технологий и изменения ландшафта угроз, прогнозирование будущих тенденций в информационной безопасности становится ключевым для предотвращения потенциальных атак. Ожидается, что в ближайшем будущем увеличится акцент на разработку и внедрение искусственного интеллекта и машинного обучения для обнаружения и нейтрализации киберугроз в реальном времени. Также предвидится рост важности защиты устройств Интернета вещей, которые становятся все более распространенными и, как следствие, могут служить дополнительными точками входа для кибератак.[3] В связи с этим, комплексная защита, включающая усиленное шифрование и аутентификацию, станет еще более важной. Кроме того, важность приобретает разработка

международных стандартов и правил поведения в киберпространстве для снижения риска масштабных киберконфликтов.

В сфере информационной безопасности постоянное развитие технологий и эволюция угроз определяют динамичный характер будущих тенденций. Адаптация к этим изменениям требует от специалистов не только реагирования на существующие вызовы, но и предвидения возможных угроз, что ведет к инновациям в методах защиты и стратегиях обеспечения безопасности.

Одним из ключевых направлений является интеграция искусственного интеллекта (ИИ) и машинного обучения в системы безопасности. Эти технологии обладают потенциалом радикально трансформировать способы обнаружения и нейтрализации киберугроз благодаря их способности анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые паттерны поведения, которые могут указывать на кибератаку.[6] Эта способность делает ИИ мощным инструментом в прогнозировании и предотвращении угроз до того, как они смогут нанести ущерб.

Также значительное внимание уделяется защите устройств Интернета вещей (IoT), число которых стремительно растет. Устройства IoT часто характеризуются недостаточным уровнем безопасности, что делает их уязвимыми для атак. В связи с этим, разработка и внедрение усовершенствованных стандартов безопасности и протоколов аутентификации становятся приоритетом для обеспечения безопасности данных и функционирования этих устройств.

Помимо технологических аспектов, ожидается усиление внимания к правовым и этическим нормам в сфере кибербезопасности. С учетом глобального характера интернета и трансграничной природы киберугроз, международное сотрудничество и разработка универсальных правовых рамок становятся критически важными для эффективного противодействия киберпреступности и защиты прав индивидов в цифровом пространстве.[1]

Наконец, учитывая растущую зависимость общества от цифровых технологий, осознание роли человеческого фактора в обеспечении информационной безопасности становится все более значимым. Это подчеркивает необходимость комплексного подхода, включающего обучение и повышение осведомленности среди пользователей о потенциальных угрозах и методах их предотвращения.

В заключение данной статьи подчеркивается, что информационная безопасность в современном мире остается одной из наиболее критических и динамично развивающихся областей. Многообразие и сложность угроз информационной безопасности требуют комплексного подхода к их предотвращению и нейтрализации, который включает в себя не только применение передовых технологий и разработку надежных технических решений, но и создание эффективной организационной культуры, направленной на защиту информации. Кроме того, особое внимание следует уделить развитию правовых и нормативных основ кибербезопасности на международном уровне, чтобы обеспечить координированное противодействие трансграничным угрозам.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.

Нижлукченко И.Д. Этичный хакинг и тестирование на проникновение: защита через наступление. введение в концепции этичного хакинга, роли и методики тестирования на проникновение для улучшения безопасности систем// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 109–114

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЭТИЧНЫЙ ХАКИНГ И ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ: ЗАЩИТА ЧЕРЕЗ НАСТУПЛЕНИЕ. ВВЕДЕНИЕ В КОНЦЕПЦИИ ЭТИЧНОГО ХАКИНГА, РОЛИ И МЕТОДИКИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ УЛУЧШЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В статье "Этичный хакинг и тестирование на проникновение: защита через наступление" освещаются ключевые концепции и методологии, лежащие в основе этичного хакинга и тестирования на проникновение, как средств обеспечения кибербезопасности. В контексте постоянно растущего числа киберугроз, авторы рассматривают эти практики как необходимые инструменты для защиты информационных систем и сетей путем активного выявления и устранения уязвимостей. Статья начинается с обзора современного ландшафта киберугроз, подчеркивая важность превентивных мер безопасности. Далее, внимание уделяется философии и методологии этичного хакинга, представляющего собой легитимное исследование систем на наличие уязвимостей с целью их последующего укрепления. Разъясняется, как этичный хакинг отличается от нелегитимного проникновения и каковы его цели и принципы.

Ключевые слова: Этичный хакинг, тестирование на проникновение, кибербезопасность, уязвимости информационных систем, стратегии обеспечения безопасности, методики киберзащиты, этические и юридические аспекты в кибербезопасности, превентивные меры безопасности, защита информационных сетей, управление киберугрозами.

ETHICAL HACKING AND PENETRATION TESTING: PROTECTION THROUGH OFFENSIVE. AN INTRODUCTION TO THE CONCEPTS OF ETHICAL HACKING, THE ROLE AND METHODS OF PENETRATION TESTING TO IMPROVE SYSTEM SECURITY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

The article "Ethical Hacking and Penetration Testing: Protection through Offensive" highlights the key concepts and methodologies underlying ethical hacking and penetration testing as a means of ensuring cybersecurity. In the context of an ever-growing number of cyber threats, the authors consider these practices as necessary tools to protect information systems and networks by actively identifying and eliminating vulnerabilities. The article begins with an overview of the modern cyber threat landscape, emphasizing the importance of preventive security

measures. Further, attention is paid to the philosophy and methodology of ethical hacking, which is a legitimate study of systems for vulnerabilities in order to strengthen them later. It explains how ethical hacking differs from illegitimate penetration and what its goals and principles are.

Keywords: Ethical hacking, penetration testing, cybersecurity, information system vulnerabilities, security strategies, cyber defense techniques, ethical and legal aspects in cybersecurity, preventive security measures, protection of information networks, cyber threat management.

В эпоху глобализированных информационных технологий и всесторонней цифровизации общества, вопросы кибербезопасности выходят на первый план. С каждым днем растет число кибератак, угрожающих личным данным пользователей, корпоративной информации и даже критически важной инфраструктуре государств. В этой связи, особую важность приобретают методики превентивного обеспечения безопасности, среди которых выделяется этичный хакинг и тестирование на проникновение. Данные подходы, ориентированные на идентификацию и устранение уязвимостей в информационных системах, представляют собой фундаментальный инструментарий в арсенале современного специалиста по кибербезопасности.

Этичный хакинг, или так называемое "белое" взломание, представляет собой практику использования методов и техник взлома для анализа безопасности информационных систем с целью их укрепления. Отличительной чертой этичного хакинга является его легитимность: действия проводятся с разрешения владельцев систем и направлены на повышение их защищенности. Ключевыми принципами этичного хакинга являются целостность, конфиденциальность и доступность информации. Специалисты в данной области обладают глубокими знаниями в области IT и кибербезопасности, а также высокой степенью этической ответственности.

Этичный хакинг является уникальным и мощным инструментом в арсенале современной кибербезопасности, воплощающим в себе комплекс философских принципов и методологических подходов. Эта практика, ориентированная на использование методов и техник взлома для идентификации и устранения уязвимостей в информационных системах, отличается от прочих подходов своей фундаментальной целью – укреплением защищенности систем.[5] Основываясь на принципах целостности, конфиденциальности и доступности информации, этичный хакинг стремится не просто выявить слабые места, но и предложить решения для их устранения, тем самым повышая уровень безопасности.

Философия этичного хакинга уходит корнями в понимание того, что для эффективной защиты системы необходимо способность мыслить как потенциальный атакующий. Это предполагает не только глубокие технические знания и навыки в области информационных технологий и кибербезопасности, но и высокую степень этической осведомленности и ответственности. Этичный хакер должен действовать с разрешения владельца системы, следуя законам и нормам, и при этом направлять свои усилия на выявление уязвимостей, которые могут быть использованы злоумышленниками.

Методология этичного хакинга включает в себя не просто применение инструментов и техник взлома, но и разработку комплексных стратегий защиты, адаптированных под конкретные условия и потребности организации. Это означает адаптацию подходов к безопасности, чтобы обеспечить защиту не только на уровне технологий, но и на уровне процессов и людей. Использование симуляций атак, анализ уязвимостей и разработка

рекомендаций по устранению обнаруженных слабостей – все это входит в компетенцию этичного хакера.

Таким образом, этичный хакинг представляет собой сложное сочетание технической экспертизы, этических принципов и стратегического планирования. Этот подход не только способствует повышению безопасности информационных систем, но и способствует формированию более широкого понимания ценности и важности информационной безопасности в современном мире.

Тестирование на проникновение, или пенетрационное тестирование, представляет собой метод оценки безопасности компьютерной системы или сети путем моделирования атаки со стороны потенциального злоумышленника.[1] Этот метод включает в себя идентификацию доступных систем, исследование возможных точек входа, попытку проникновения и анализ полученных результатов для выявления уязвимостей. Тестирование на проникновение может быть проведено с различными уровнями знаний о системе: от полного незнания до полного понимания внутренней структуры тестируемой системы. Этот процесс не только выявляет слабые места, но и помогает в разработке рекомендаций по усилению защиты.

Тестирование на проникновение является одним из ключевых элементов стратегии обеспечения кибербезопасности, представляя собой комплексный и многоуровневый подход к выявлению уязвимостей в информационных системах и сетях. Этот процесс эмулирует действия потенциального атакующего с целью обнаружения и последующего устранения уязвимостей, которые могут быть использованы для незаконного проникновения или нанесения вреда системе. Суть тестирования на проникновение заключается не просто в поиске слабых мест, но и в понимании того, как эти слабые места могут быть использованы в реальных атаках, а также в разработке мер по их нейтрализации.

Основная стратегия тестирования на проникновение предполагает целенаправленное и планомерное исследование информационной системы с использованием различных методов и техник, варьируя от автоматизированного сканирования до ручного тестирования и анализа. Этот процесс требует от исполнителей не только глубоких технических знаний и практических навыков, но и креативного подхода к решению задач, поскольку каждая система уникальна и может требовать индивидуального подхода к тестированию.

Тактика тестирования на проникновение включает в себя подготовительный этап, на котором определяются цели тестирования, выбираются методы и инструменты, а также устанавливаются рамки допустимых действий во избежание непреднамеренного вреда тестируемым системам. Затем следует этап активного сканирования и идентификации потенциальных точек входа, который позволяет составить карту уязвимостей. После этого осуществляется непосредственное тестирование на проникновение с целью эксплуатации найденных уязвимостей, что дает представление о реальных рисках безопасности. Финальный этап предполагает анализ полученных данных, подготовку отчета с детальным описанием обнаруженных проблем и рекомендаций по их устранению.[3]

Тестирование на проникновение не является однократной акцией, а представляет собой часть непрерывного процесса управления кибербезопасностью, требующего регулярного повторения для эффективной защиты от новых и эволюционирующих угроз. Это стратегический инструмент, который позволяет организациям не только обнаруживать и

устранять существующие уязвимости, но и формировать устойчивую культуру безопасности, адаптируемую к постоянно меняющемуся ландшафту угроз.

В процессе этичного хакинга и тестирования на проникновение задействованы различные специалисты, каждый из которых играет уникальную роль в обеспечении кибербезопасности информационных систем. Эти профессионалы, работая как единая команда, применяют широкий спектр методик и стратегий для выявления и устранения уязвимостей, что требует от них не только глубоких технических знаний, но и понимания целей и бизнес-процессов организации.

Среди ключевых участников процесса этичного хакинга и тестирования на проникновение выделяются аудиторы безопасности, которые отвечают за оценку соответствия системы стандартам и требованиям кибербезопасности, и специалисты по кибербезопасности, которые непосредственно занимаются идентификацией уязвимостей и разработкой рекомендаций по их устранению.[4] Кроме того, в этот процесс могут быть вовлечены системные администраторы и разработчики, которые обеспечивают техническую поддержку тестирования и реализацию предложенных улучшений безопасности.

Методики, используемые в ходе этих действий, варьируются от автоматизированного сканирования систем на предмет известных уязвимостей до ручных тестов и анализа для выявления неочевидных слабых мест. Особое внимание уделяется анализу данных, получаемых в ходе тестирования, что требует от специалистов не только технических знаний, но и аналитических навыков для правильной интерпретации результатов.

Применяемые методики направлены на всестороннее исследование системы, начиная от внешнего периметра и заканчивая внутренними компонентами, что позволяет обеспечить комплексную защиту. Важной частью работы является и разработка стратегий по обеспечению безопасности, включающих в себя как немедленные меры по устранению обнаруженных уязвимостей, так и долгосрочные планы по повышению уровня безопасности системы в целом.

Эта командная и мультидисциплинарная работа требует от всех участников не только высокой квалификации и профессионализма, но и способности к творческому подходу в решении задач кибербезопасности. Использование разнообразных методик позволяет подходить к вопросам безопасности комплексно, что в свою очередь способствует созданию более защищенной и устойчивой к атакам информационной среды.

Этические и юридические аспекты этичного хакинга и тестирования на проникновение играют критически важную роль в обеспечении, чтобы эти практики проводились ответственно и в соответствии с законодательством. Основываясь на принципе, что цель этих действий заключается в улучшении безопасности, а не в нарушении конфиденциальности или целостности данных, профессионалы в этой области должны строго следовать как этическим, так и юридическим стандартам.

Важным этическим принципом в этих областях является получение явного разрешения от владельцев или управляющих системами перед проведением любых тестов на проникновение или хакинга.[3] Это гарантирует, что все действия выполняются в рамках согласованных условий и не превышают предоставленные полномочия. Более того, специалисты обязаны сохранять конфиденциальность всей полученной в ходе тестирования

информации, а также действовать с целью минимизации любого возможного вреда для тестируемой системы.

С юридической точки зрения, действия, связанные с этичным хакингом и тестированием на проникновение, могут натолкнуться на различные законодательные ограничения, связанные с несанкционированным доступом к компьютерным системам, злоупотреблением владельческими данными и другими аспектами кибербезопасности. В разных юрисдикциях существуют различные нормы и законы, регулирующие эти вопросы, и профессионалы должны обладать знаниями актуальных законодательных требований и следовать им для избежания юридических последствий.

Кроме того, этичный хакинг и тестирование на проникновение требуют четкого определения рамок и целей тестирования, чтобы убедиться, что все действия направлены на достижение конструктивных результатов в области безопасности. Это включает в себя документирование всех шагов и процедур, а также разработку и внедрение мер по устранению выявленных уязвимостей.

Таким образом, соблюдение этических и юридических норм не только обеспечивает легитимность и ответственность процесса этичного хакинга и тестирования на проникновение, но и поддерживает доверие между всеми заинтересованными сторонами, включая компании, их клиентов и общественность в целом. Это создает основу для ответственного и эффективного применения этих практик в рамках общей стратегии кибербезопасности.

Этичный хакинг и тестирование на проникновение являются неотъемлемой частью стратегии обеспечения кибербезопасности в современном мире. Они позволяют не просто реагировать на угрозы, но и активно предотвращать их, используя методы и техники, аналогичные тем, что применяют злоумышленники. Таким образом, "защита через наступление" обеспечивает глубокое понимание угроз и разработку эффективных мер по защите информационных систем от возможных атак. Важно, что все действия в рамках этичного хакинга и тестирования на проникновение проводятся с соблюдением высоких этических норм и юридических требований, что делает эти практики не только эффективными, но и легитимными инструментами защиты киберпространства.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2

4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Чуков Ю.В. Модернизация системы теплоснабжения промышленных предприятий // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 115–125

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 697

МОДЕРНИЗАЦИЯ СИСТЕМЫ ТЕПЛОСНАБЖЕНИЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Чуков Ю.В.
ФГБОУ ВО «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ», Самара, Россия, (443100, Самарская область, город Самара, Молодогвардейская ул., д.244), e-mail: yura2183@mail.ru

В данной работе представлен обзор на статьи, где рассмотрены самые современные методы повышение энергоэффективности и энергосбережения на промышленных предприятиях путем модернизации систем теплоснабжения и использование вторичных энергетических ресурсов.

Ключевые слова: Котельная, модернизация, реконструкция, энергоэффективность, теплоснабжение промышленных предприятий.

MODERNIZATION OF THE HEAT SUPPLY SYSTEM OF INDUSTRIAL ENTERPRISES

Chukov Yu.V.
SAMARA STATE TECHNICAL UNIVERSITY, Samara, Russia, (443100, Samara region, Samara, Molodogvardeyskaya str., 244), e-mail: yura2183@mail.ru

This paper provides an overview of articles that consider the most modern methods of improving energy efficiency and energy saving in industrial enterprises through the modernization of heat supply systems and the use of secondary energy resources.

Keywords: Boiler house, modernization, reconstruction, energy efficiency, heat supply of industrial enterprises.

Высокий уровень энергоемкости и потребности в модернизации экономики делают задачу повышения энергоэффективности особенно актуальной для России. Стремление к повышению конкурентоспособности промышленности и улучшению состояния окружающей среды диктует необходимость обновления и модернизации тепловых установок и сетей.

Фактический износ и устаревшие технологии в тепловом секторе промышленности приводят к тому, что существующие системы теплоснабжения не могут обеспечить необходимой энергоэффективности и соответствовать современным эксплуатационным стандартам. Поэтому модернизация котельных, оборудования и тепловых сетей становится неотложной задачей для обеспечения надежного и эффективного теплоснабжения, а также для снижения негативного воздействия на окружающую среду.

Исследование модернизации системы теплоснабжения с использованием утилизации тепловой энергии при ресурсных испытаниях газотурбинных двигателей не только поможет улучшить состояние систем теплоснабжения, но также способствует решению важных

проблем энергосбережения, экологической безопасности и повышения конкурентоспособности промышленного сектора.

Модернизация котельных играет ключевую роль в повышении эффективности и безопасности работы, а также в уменьшении эксплуатационных расходов. Ниже приведен список случаев, когда модернизация оборудования необходима, включает важные аспекты, которые определяют не только работоспособность котельной, но и ее воздействие на окружающую среду.

1. *Износ оборудования:* физический и моральный износ оборудования снижает его эффективность и безопасность, а также увеличивает риск аварийных ситуаций, что делает модернизацию необходимой мерой.
2. *Потребление электроэнергии:* высокий расход электроэнергии на выработку тепловой энергии указывает на неэффективность и потребность в использовании более современных и энергоэффективных технологий.
3. *Перебои в температурных режимах:* нестабильность температурных режимов может привести к простою оборудования и неустойчивости в подаче тепла, что негативно влияет на комфорт и производственные процессы.
4. *Смена вида топлива***:** переход с одного вида топлива на другой требует соответствующей адаптации оборудования, чтобы обеспечить безопасность и эффективность процесса.
5. *Отсутствие возможности постройки нового источника***:** в ситуациях, когда невозможно построить новый источник теплоснабжения, модернизация оборудования позволяет улучшить производительность и безопасность существующей системы.
6. *Экологические аспекты***:** увеличение выбросов вредных веществ требует принятия мер по снижению негативного воздействия на экосистему через модернизацию оборудования с целью сокращения загрязнений.

Этот перечень отражает важные факторы, которые делают модернизацию котельных необходимой и актуальной в контексте обеспечения эффективности, безопасности и экологической устойчивости систем теплоснабжения.

Реконструкция котельной представляет собой важный процесс, который может включать как частичную, так и полную замену изношенного оборудования на новое с целью улучшения работы теплового источника. Такие действия помогают оптимизировать работу системы, повысить эффективность установки и снизить эксплуатационные затраты.

Многие котельные, которые до сих пор используют твердое или жидкое топливо, имеют потенциал для перехода на более современное и эффективное использование природного газа. Обновление котельных поможет не только снизить расходы на ремонт и эксплуатацию, но и приведет оборудование в соответствие с современными стандартами безопасности и энергоэффективности.

Важно отметить, что моральное и физическое старение оборудования котельной может привести к частым поломкам и повышенным затратам на ремонт. Поэтому комплексная работа по реконструкции котельной становится все более актуальной с течением времени. Эта мера позволяет не только повысить надежность работы системы, но и снизить тарифы на

теплоснабжение для потребителей в результате улучшения эффективности и снижения эксплуатационных расходов.

Своевременная реконструкция котельной является важным шагом в повышении тепловой эффективности объекта. Замена устаревшего оборудования на современное более мощное с высоким КПД может значительно улучшить производительность котельной и снизить расходы на энергоносители. Модернизация систем подачи топлива и теплоносителя также играет важную роль в оптимизации работы установки.

Современные котлы и вспомогательное оборудование, устанавливаемые в процессе реконструкции, обладают возможностью интеграции с компьютерными системами, что обеспечивает не только более точный контроль над процессами, но и увеличивает уровень автоматизации работы котельной. Это позволяет снизить вмешательство человеческого фактора и улучшить управление параметрами работы оборудования.

Благодаря своевременной реконструкции котельной улучшается качество услуг по теплоснабжению абонентов, а также сокращается вредное воздействие на окружающую среду за счет снижения выбросов. Все эти меры в совокупности способствуют эффективной и экологически безопасной работе котельной.

Реконструкция котельной имеет ключевое значение для обеспечения энергоэффективности и стабильной работы объекта. Виды работ при реконструкции котельной весьма разнообразны и включают в себя современные технологии и методы, которые позволяют значительно улучшить эффективность системы отопления.

Применение газопоршневых машин, переход к водогрейному режиму котлов и внедрение альтернативных видов топлива не только повышают энергетическую эффективность, но и способствуют сокращению затрат на эксплуатацию. Другие модернизационные работы с котельным оборудованием, такие как замена теплоснабжающих путей и внедрение индивидуальных комплексных автоматизированных систем управления, также играют важную роль в оптимизации процессов и снижении расходов.

Результаты проведенной реконструкции впечатляющие: повышение КПД объекта до 93%, увеличение тепловой мощности, снижение расхода топлива и энергопотребления. Это не только сокращает затраты на эксплуатацию и обслуживание в ближайшие годы, но также способствует увеличению экологической дружелюбности объекта за счет использования вторичных энергетических ресурсов.

Реконструкция котельной - это инвестиция в будущее, которая не только повышает эффективность работы системы отопления, но и сокращает негативное воздействие на окружающую среду. Внедрение современных технологий и методов позволяет обеспечить стабильность и эффективность работы котельной даже в самые суровые условия, что является ключевым фактором для комфортной и безопасной эксплуатации объекта.

Основная часть

Исходя из экономической точки зрения, централизованное теплоснабжение на базе теплоэлектроцентралей (ТЭЦ) оказывается более выгодным в сравнении с использованием малых персональных котельных для обогрева производственных помещений.

Предлагаемые преимущества централизованного теплоснабжения с помощью ТЭЦ включают:

- когенерация: одновременная генерация тепла и электроэнергии на ТЭЦ с высоким коэффициентом полезного действия (КПД) повышает эффективность процесса;
- экономичность в эксплуатации: масштаб производства на ТЭЦ позволяет использовать более экономичные термодинамические режимы, повышая эффективность процесса генерации тепла;
- себестоимость: благодаря централизованной логистике, меньшим накладным расходам и более эффективной производственной системе ТЭЦ обеспечивает более низкую себестоимость производимой тепловой энергии по сравнению с автономными источниками тепла.

Несмотря на все эти преимущества, распределительные сети теплоснабжения представляют значительную проблему. Получившая широкое распространение неэффективная теплоизоляция и плачевное состояние тепловых сетей приводят к катастрофическим потерям тепла в процессе передачи — до 60% в некоторых случаях. Эти потери тепла обременяют финансово потребителей, которые вынуждены оплачивать как утраченную энергию, так и необходимость модернизации теплосетей и замену оборудования.

В целом, централизованное теплоснабжение на базе ТЭЦ представляет экономическую и экологическую выгоду, но эффективность такой системы сильно зависит от состояния распределительных сетей и необходимости их модернизации. Следовательно, при выборе между автономными системами и централизованным подходом важно учитывать все аспекты: преимущества ТЭЦ, проблемы распределительных сетей и необходимость повышения эффективности теплоснабжения.

В работе [1] рассматривается вопрос правильной оценке показателей энергетической эффективности и потенциала энергосбережения. Большинство существующих методик оценки показателей энергетической эффективности носят ограниченный характер и позволяют произвести оценку только одного или нескольких показателей, не предусматривают увязку всех показателей в единое целое. Кроме того, отсутствует критерий оценки энергетической эффективности, единый для всех составляющих систем теплоснабжения. Перспективными направлениями современных исследований в области систем теплоснабжения становятся совершенствование способов оценки энергетической эффективности систем теплоснабжения посредством использования научно обоснованного критерия энергетической эффективности системы теплоснабжения промышленных предприятий и создание унифицированных методик и алгоритма оценки показателей энергетической эффективности систем теплоснабжения различного состава и устройства. Отдельное внимание уделяется оценке достоверности исходных данных. Выполнение этой оценки возможно с помощь корреляционного метода. На практике широко применяется корреляционно-регрессионный анализ для прогнозирования потребления тепловой энергии. Этот подход можно использовать и при оценке достоверности исходных данных с использованием шкалы Чеддока. В ходе исследований применены методы конструктивных и поверочных расчетов, экспериментальные и аналитические исследования, метод корреляционного анализа, статистические методы исследования. В результате исследований разработана единая, обобщенная методика оценки показателей энергетической эффективности системы теплоснабжения предприятия. Создан алгоритм, позволяющий дать комплексную оценку энергетической эффективности системы теплоснабжения промышленного предприятия и оценить потенциал энергосбережения.

Анализ ориентировочного потенциала энергосбережения в области производства и преобразования энергетических ресурсов показал, что его наибольшее значение приходится на генерацию и преобразование тепловой энергии.

В работе [1] проводится анализ исследования в области оценки энергетической эффективности систем теплоснабжения промышленных предприятий. Предпринимается попытка разработать унифицированные методики и алгоритмы оценки показателей энергетической эффективности различных систем теплоснабжения. Также отмечается беспокойство по поводу отсутствия единого критерия оценки энергетической эффективности, применимого ко всем аспектам систем теплоснабжения.

Автор также рассматривает применение корреляционного метода для оценки достоверности исходных данных и подчеркивает значимость аналитических и экспериментальных методов в контексте разработки методики оценки энергетической эффективности.

Исследование также касается анализа потенциала энергосбережения, сосредотачиваясь на генерации и преобразовании тепловой энергии.

Это исследование представляется информативным и ценным для развития методик оценки энергетической эффективности систем теплоснабжения, поскольку оно охватывает методы анализа и корреляционной проверки данных, а также предоставляет единые критерии оценки.

Оценка энергоэффективности систем теплоснабжения является важным этапом в улучшении работы промышленных предприятий. Недостаток общепринятых критериев и методологий подчеркивает необходимость разработки более совершенных подходов к оценке энергетической эффективности.

Проведение контрольных испытаний, сбор и анализ данных, разработка топливно-энергетического баланса и принятие мер по энергосбережению являются неотъемлемой частью этого процесса. Важно уделить внимание основным показателям энергоэффективности, таким как удельный расход энергии, степень загрузки оборудования, затраты и потери тепла.

Контрольно-балансовые испытания позволяют получить дополнительную информацию о работе системы теплоснабжения и сделать более точные оценки показателей. Развитие более точных методов оценки энергоэффективности систем теплоснабжения позволит эффективнее использовать энергетические ресурсы и снизить затраты на энергию, что является важным шагом в направлении устойчивого развития промышленности.

Действительно, отсутствие единого физико-математического аппарата для оценки критерия энергетической эффективности представляет собой значительное препятствие для комплексной оценки систем теплоснабжения. Различные методики оценки эффективности отопительных систем, теплогенерирующих объектов и сетей теплоснабжения усложняют сравнение и оценку эффективности систем в целом.

Исследование, описанное в работе [1], выглядит важным в контексте разработки унифицированной методики оценки энергетической эффективности. Предложенный критерий энергетической эффективности для систем теплоснабжения промышленных предприятий представляет собой значительный прогресс. Он позволяет оценить существующее состояние систем теплоснабжения, облегчает анализ и планирование мероприятий по повышению

эффективности и способствует формированию технико-экономического обоснования для программы энергосбережения.

Однако для успешной реализации предложенной методики важно убедиться в ее адаптации к различным типам систем теплоснабжения и промышленных предприятий, а также ее пригодности для учета всех аспектов энергопотребления.

Данное исследование является важным шагом в решении проблемы отсутствия единого физико-математического аппарата для оценки критерия энергетической эффективности, и его применение может стать значительным преимуществом для повышения эффективности систем теплоснабжения промышленных предприятий.

В работе [2] видно, что модернизация открытых систем теплоснабжения на закрытую схему представляет сложную задачу, требующую значительных работ, времени и инвестиций. Из-за этих факторов проекты модернизации часто сталкиваются с низкой экономической эффективностью, что затрудняет их реализацию.

Для успешной модернизации систем теплоснабжения в данных условиях ключевым фактором является повышение энергетической эффективности при минимизации капитальных затрат. В данном контексте важны различные технические решения, предполагающие использование альтернативных методов модернизации, например, индивидуальных тепловых пунктов с пиковым источником тепла.

Установленное законодательством требование о переходе к закрытым системам теплоснабжения с 1 января 2022 года, а также устаревшее состояние основных фондов отрасли, делают модернизацию систем теплоснабжения необходимой. Одним из ключевых документов, определяющих цели и принципы развития отрасли, являются схемы теплоснабжения городов, в которых разрабатываются материалы по обоснованию эффективной и безопасной работы систем.

Для повышения экономической эффективности рассматриваются альтернативные модернизационные варианты, включая автоматизацию элеваторных узлов и использование струйных аппаратов. Эти решения направлены на обеспечение энергетической эффективности при снижении капитальных затрат и повышении управляемости систем теплоснабжения

Из приведенной информации в работе [2] очевидно, что решение о выборе приоритетного варианта модернизации системы теплоснабжения должно опираться на технико-экономическое обоснование, учитывающее многочисленные факторы. Существует множество параметров, которые необходимо учесть при сравнении альтернативных вариантов модернизации, таких как способы регулирования отпуска тепла, тип источника теплоснабжения, уровень тепловых нагрузок и существующие схемы присоединения потребителей.

Необходимость модернизации открытых систем теплоснабжения промышленных предприятий становится ключевой из-за старения оборудования, роста затрат на обслуживание и ремонт, увеличения потерь тепловой энергии, расходов топлива, ухудшения экологической обстановки и увеличения себестоимости производства электроэнергии и тепла. Однако реализация подобных проектов требует сбора, анализа и обработки большого объема данных, а также учета многочисленных факторов, связанных с межотраслевой синхронизацией работ.

Учитывая сложность проблемы модернизации систем теплоснабжения, несомненно, что адекватное технико-экономическое обоснование выбора технических решений играет

ключевую роль в успешной реализации проектов по переходу открытых систем теплоснабжения на закрытую схему. Комплексная модернизация открытых систем теплоснабжения, лежащая в основе представленного подхода, сможет значительно повысить эффективность потребления тепловой энергии и стимулировать последующие изменения в отрасли.

В работе [3] выбранная реконструкция котельной, направленная на повышение энергоэффективности и снижение эксплуатационных расходов, представляется значительным изменением для системы теплоснабжения в бизнес-парке. Установка стальных котлов Unical Modal, гидравлической стрелки Sinus, трехходовых кранов Vexve, погодозависимой автоматики и нового дымохода из нержавеющих труб обещает улучшить надежность и эффективность системы.

Данная реконструкция позволит сократить расход дизельного топлива за счет повышения эффективности работы котельной, а также снизить выброс вредных веществ в атмосферу благодаря более эффективному сгоранию и мониторингу параметров работы системы. Погодозависимая автоматика также способствует оптимизации работы в зависимости от внешних условий, что может снизить излишние расходы энергоресурсов.

Рисунок 1 – Котельная до реконструкции

Рисунок 2 – Котельная после реконструкции

В целом, данные технические изменения представляют собой важный шаг в обеспечении более устойчивой и эффективной работы системы теплоснабжения, приводя к снижению эксплуатационных затрат и улучшению экологических характеристик работы котельной.

В работе [4] рассматривается применение конденсационных газовых котлов. Конденсационные газовые котлы представляют собой одни из наиболее экономичных и эффективных систем отопления. Они имеют выше коэффициент полезного действия (КПД) на 10–15% в сравнении с традиционными газовыми котлами. За счет использования конденсации водяных паров из продуктов сгорания, конденсационные котлы обеспечивают уровень КПД до 95–96%. Для их работы требуется подача теплоносителя с низкой температурой, что обеспечивает конденсационный режим.

Однако, применение конденсационных котлов сталкивается с определенными проблемами, включая организацию аэродинамических режимов работы дымоходов при низких температурах, образование обледенения неизолированных участков и пропуск влаги в дымовые трубы. Для предотвращения этих проблем необходимо обеспечить теплоизоляцию дымовых труб и выходных участков. Уклон газохода к котлу через конденсатоотводный узел также важен для отвода конденсата. Для конденсационных котлов рекомендуется использование газоходов и дымовых труб из полипропилена и нержавеющей стали для обеспечения долговечности и надежности работы системы

В работе [5] рассматривается состояние энергетики России и обозначаются возможные пути повышения устойчивости через внедрение новых энергоблоков на основе парогазового цикла. Обзор технологических схем парогазовых установок котлами-утилизаторами является значимым шагом в этом направлении.

Подход, основанный на создании высокоэкономичных энергоблоков с супер сверхкритическими параметрами пара для удовлетворения необходимых графиков нагрузки, также привлекает внимание к приоритету автоматизации технологического процесса.

Важными аспектами являются снижение удельных затрат на производство электрической и тепловой энергии, повышение надежности и защиты окружающей среды от вредного воздействия.

Имеющиеся резервы природного газа делают комбинированный цикл (ПГУ) мощным и перспективным решением для российской энергетики, учитывая его высокую эффективность по сравнению с традиционными паросиловыми установками. Определение эффективности работы отдельных энергосистем через себестоимость электроэнергии, сроки ввода объектов и удельные затраты на оборудование электростанций также актуальны и важны для принятия достоверных решений в сфере энергетики.

Подчеркивается, что предложенный вариант строительства энергоблоков по комбинированному циклу (ПГУ) может значительно повысить энергетическую стабильность, особенно в контексте возрастающего спроса на энергию и необходимости обеспечения устойчивого и эффективного производства электроэнергии.

Котлы-утилизаторы различаются по компоновке, тепловым схемам и параметрам. Подробное описание различных аспектов проектирования и функционирования таких котлов демонстрирует важность оптимизации процессов для повышения эффективности производства энергии и устойчивости работы систем.

Использование горизонтальных или вертикальных котлов-утилизаторов с тепловыми схемами барабанного типа и спиральным оребрением поверхностей теплообмена является технически продвинутым решением для сокращения металлоемкости и увеличения эффективности теплообмена. Важно отметить внедрение газовых подогревателей конденсата для охлаждения дымовых газов и поддержания оптимальной температуры.

Наличие системы рециркуляции подогретого конденсата, дожигающих устройств для стабилизации параметров или увеличения производительности котлов-утилизаторов демонстрирует стремление к оптимизации энергетических процессов при проектировании таких установок. Учет требований к горелочным устройствам и соблюдение технических условий играют ключевую роль в обеспечении безопасной и эффективной работы энергетических систем.

Эти современные методы и технологии позволяют значительно повысить КПД производства электроэнергии и эффективность работы энергетических установок, что важно для обеспечения устойчивого функционирования энергетической отрасли.

Заключение

Исследования показывают - модернизация систем теплоснабжения промышленных предприятий является перспективным направлением развития. Для успешной реализации этой задачи необходимо учитывать множество факторов. Среди них:

1. Модернизация центральных тепловых пунктов (ЦТП) и индивидуальных тепловых пунктов (ИТП), что позволит повысить эффективность и надежность работы системы.
2. Модернизация открытых систем теплоснабжения для оптимизации процессов и снижения потерь тепла.
3. Модернизация или реконструкция действующих котельных с установкой современного оборудования для повышения энергоэффективности.

4. Применение конденсационных газовых котлов, обеспечивающих высокий коэффициент полезного действия и эффективное использование топлива.
5. Внедрение энергоблоков на основе парогазового цикла для повышения энергетической устойчивости и эффективности производства электроэнергии.

Список литературы

1. А.С.Краснов, К.К.Ким «Оценка энергоэффективности систем теплоснабжения промышленных предприятий» Петербургский государственный университет путей сообщения Императора Александра I (ПГУПС),г. Санкт-Петербург, Российская Федерация, 2021
2. И.Г.Черненко «Альтернативные варианты модернизации открытых систем теплоснабжения» изд. Энергосбережение и энергоэффективность, 2020
3. Куликова С.Е., Готулева Ю.В., Суконкина Ю.Ю «Повышение эффективности работы котельной» Нижегородский государственный архитектурно-строительный университет Нижний Новгород, 2018
4. Сборник работ аспирантов и студентов – сотрудников научно-исследовательской лаборатории «теплоэнергетические системы и установки» г. Ульяновск, 2019
5. С.Н. Хуторненко, И.Д. Фурсов, Г.П. Пронь «Котлы-утилизаторы, предназначенные для работы в составе энергоблоков пгу» ФГБОУ ВПО «Алтайский государственный технический университет им. И.И. Ползунова», кафедра «Котло- и реакторстроения», г. Алтай, 2013
6. 67-я научно-техническая конференция учащихся, студентов и магистрантов, 18-23 апреля, Минск : сборник научных работ : в 4 ч. Ч. 1 / Белорусский государственный технологический университет. - Минск : БГТУ, 2016. - 308 с.
7. Энергетическая стратегия Российской Федерации на период до 2035 года (Распоряжение Правительства Российской Федерации от 9 июня 2020 г. № 1523-р).
8. Об утверждении порядка определения нормативов удельного расхода топлива при производстве электрической и тепловой энергии (вместе с «Порядком определения нормативов удельного расхода топлива при производстве электрической и тепловой энергии»). Приказ Минэнерго России от 30.12.2008 № 323 (ред. от 30.11.2015). –
9. СП 50.13330.2012. Тепловая защита зданий. – Москва : Минрегион России, 2012.
10. СП 60.13330.2016. Отопление, вентиляция и кондиционирование воздуха. – Москва : Минстрой России, 2016.
11. Середкин А. А. Методика и критерий оценки энергоэффективности систем теплоснабжения / А. А. Середкин. Текст : непосредственный // Научно-технические ведомости СПбГПУ. – 2017. – Т. 23. – № 1. – С. 27–35.
12. Практическое пособие по выбору и разработке энергосберегающих проектов: в семиразделах, под общей ред. О. Л. Данилова, П. А. Костюченко. – Москва : ЗАО «Технопромстрой», 2006. –688 с.
13. Данилов Н. И. «Основы энергосбережения» / Н. И. Данилов, Я. М. Щелоков. – Екатеринбург : Уральский гос. техн. ун-т, 2005. –564 с. –Текст : непосредственный
14. Палей Е.Л. «Котельные. Нормативные требования и практические рекомендации при проектировании», 2010 г. – 117 с
15. Соколов Б.А. «Газовое топливо и газовое оборудование котельных», 2008 г. – 64 с.

16. СП 89.13330.2016 Котельные установки. Актуализированная редакция СНиП II-35-76

References

1. A.S.Krasnov, K.K.Kim "Assessment of energy efficiency of heat supply systems of industrial enterprises" St. Petersburg State University of Railways of Emperor Alexander I (PGUPS), St. Petersburg, Russian Federation, 2021
2. I.G.Chernenko "Alternative options for modernization of open heat supply systems" ed. Energy saving and energy efficiency, 2020
3. Kulikova S.E., Gotuleva Yu.V., Sukonkina Yu.Yu. "Improving the efficiency of the boiler room" Nizhny Novgorod State University of Architecture and Civil Engineering Nizhny Novgorod, 2018
4. Collection of works by graduate students and students – employees of the research laboratory "Thermal power systems and installations" Ulyanovsk, 2019
5. S.N. Khutornenko, I.D. Fursov, G.P. Pron "Waste heat boilers designed to work as part of the power units of the PSU "FGBOU VPO"Altai State Technical University named after I.I. Polzunova", Department of Boiler and Reactor Engineering, Altai, 2013
6. 67th Scientific and Technical Conference of students, undergraduates and undergraduates, April 18-23, Minsk : collection of scientific papers : at 4 p.m. 1 / Belarusian State Technological University. - Minsk : BSTU, 2016. - 308 p.
7. Energy Strategy of the Russian Federation for the period up to 2035 (Decree of the Government of the Russian Federation dated June 9, 2020 No. 1523-r).
8. On approval of the procedure for determining the standards of specific fuel consumption in the production of electric and thermal energy (together with the "Procedure for determining the standards of specific fuel consumption in the production of electric and thermal energy"). Order of the Ministry of Energy of the Russian Federation dated 12/30/2008 No. 323 (ed. dated 11/30/2015). –
9. SP 50.13330.2012. Thermal protection of buildings. – Moscow : Ministry of Regional Development of Russia, 2012.
10. SP 60.13330.2016. Heating, ventilation and air conditioning. – Moscow : Ministry of Construction of Russia, 2016.
11. Seredkin A. A. Methodology and criterion for evaluating the energy efficiency of heat supply systems / A. A. Seredkin. Text : direct // Scientific and Technical bulletin of St. Petersburg State University. – 2017. – Vol. 23. – No. 1. – pp. 27-35.
12. Practical guide to the selection and development of energy-saving projects: in seven sections, under the general editorship of O. L. Danilova, P. A. Kostyuchenko. – Moscow : Technopromstroy CJSC, 2006. -688 p.
13. Danilov N. I. "Fundamentals of energy saving" / N. I. Danilov, Ya. M. Shchelokov. – Yekaterinburg : Ural State Technical University. Univ., 2005. -564 p. –Text : direct
14. Paley E.L. "Boiler rooms. Regulatory requirements and practical recommendations for design", 2010 – 117 p
15. Sokolov B.A. "Gas fuel and gas boiler equipment", 2008 – 64 p.
16. SP 89.13330.2016 Boiler installations. Updated version of SNiP II-35-76

Подлесных А.А. Повышение энергоэффективности объектов жилищно-коммунального комплекса // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 126–133

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 332.8

ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ ОБЪЕКТОВ ЖИЛИЩНО-КОММУНАЛЬНОГО КОМПЛЕКСА

Подлесных А.А.
ФГАОУ ВО «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА», Москва, Россия, (127055, город Москва, ул. Образцова, д.9 стр.9), e-mail: toni481@mail.ru

Данная статья рассматривает важную тему – энергоэффективность в жилищно-коммунальном хозяйстве. Автор обсуждает преимущества и выгоды внедрения энергоэффективных технологий и подходов в данной сфере. В статье акцентируется внимание на необходимости системной модернизации и инновационном развитии отечественных организаций жилищно-коммунального хозяйства. Энергоснабжение объектов жилищно-коммунального хозяйства и инфраструктуры—это всегда анализ потребностей заказчиков и предоставление эффективного комплексного решения поставленной задачи в общей системе менеджмента. Даны классы энергоэффективности жилых домов с величинами отклонения от нормативных показателей. Предлагаются технические решения по повышению энергоэффективности, позволяющие получить значительную экономию тепловой энергии (до 30-40%) при сроке окупаемости 2-3 года.

Ключевые слова**:** Энергоэффективность, энергосбережение, классы энергоэффективности, удельное энергопотребление, технические решения, окружающая среда, инновации, рабочие места, инвестиции, услуги.

IMPROVING THE ENERGY EFFICIENCY OF HOUSING AND COMMUNAL COMPLEX FACILITIES

Podlesnykh A.A.
RUSSIAN UNIVERSITY OF TRANSPORT, Moscow, Russia, (127055, Moscow, Obraztsova str., 9, bldg. 9), e-mail: toni481@mail.ru

This article examines an important topic – energy efficiency in housing and communal services. The author discusses the advantages and benefits of implementing energy-efficient technologies and approaches in this area. The article focuses on the need for systemic modernization and innovative development of domestic housing and communal services organizations. Energy supply of housing and communal services and infrastructure facilities is always an analysis of customer needs and the provision of an effective integrated solution to the task in the overall management system. The energy efficiency classes of residential buildings with the values of deviation from the normative indicators are given. Technical solutions are proposed to improve energy efficiency, allowing for significant savings in thermal energy (up to 30-40%) with a payback period of 2-3 years.

Keywords: Energy efficiency, energy saving, energy efficiency classes, specific energy consumption, technical solutions, environment, innovations, jobs, investments, services.

Проблемы энергоэффективности и устойчивости энергетической системы остаются одними из наиболее актуальных вызовов современного мира. Сегодняшние вызовы в жилищно-коммунальном секторе России связаны не только с обеспечением населения качественными услугами по тепло- и электроснабжению, но и с соблюдением мировых стандартов в области энергоэффективности и снижения негативного воздействия на

окружающую среду [1]. Переход к более устойчивому и эффективному потреблению энергии в жилищном секторе становится необходимостью как с точки зрения обеспечения национальной энергетической безопасности, так и с позиции снижения вредного выброса парниковых газов.

Современное жилищно-коммунальное хозяйство России сталкивается с рядом серьезных проблем, связанных с энергопотреблением и энергоэффективностью. Эти проблемы оказывают значительное воздействие на экономику, экологию и качество жизни населения. В данной статье мы рассмотрим основные аспекты этих проблем, а также перспективы их решения.

Важной проблемой является устаревшее оборудование и инфраструктура. Большая часть жилищного фонда России построена много десятилетий назад и не соответствует современным требованиям энергоэффективности. Устаревшие системы отопления, вентиляции и кондиционирования воздуха не только потребляют больше энергии, но и снижают комфорт жильцов.

Другим значительным фактором является низкая энергоэффективность зданий и домов [2]. Плохая теплоизоляция, старые оконные и дверные конструкции, отсутствие современных систем управления отоплением - все это приводит к избыточным расходам энергии. Теплопотери зданий оцениваются миллионами кубических метров газа, что создает ненужную нагрузку на энергосистему страны.

Также важно отметить отсутствие сознательного потребления энергии. Несмотря на потенциал для экономии, население не всегда осознает важность энергосбережения. Это проявляется в необоснованных расходах на освещение, отопление и бытовые приборы.

Поэтому осознанное внедрение энергоэффективных технологий и подходов в жилищно-коммунальное хозяйство имеет ряд преимуществ и выгод для общества.

Первое преимущество, как уже упоминалось, связано с экономией затрат на энергию и коммунальные услуги. Граждане могут значительно снизить свои расходы, что особенно актуально в условиях растущих тарифов на энергоресурсы. Более того, сокращение потребления энергии и ресурсов позволяет снизить зависимость от их импорта, что способствует укреплению энергетической безопасности.

Второе преимущество энергоэффективности в ЖКХ связано с экологической составляющей. Меньшее потребление энергии и уменьшение выбросов загрязняющих веществ существенно снижает негативное воздействие на окружающую среду и улучшает качество жизни людей. Это особенно важно в городах, где концентрация выбросов часто достигает высоких уровней, и где стремятся к созданию здоровой и экологически чистой среды.

Третье преимущество заключается в экономическом и социальном развитии. Внедрение энергоэффективных систем и технологий позволяет создавать новые рабочие места, развивать инновационные отрасли и привлекать инвестиции. Это способствует снижению безработицы и повышению уровня жизни граждан. Более того, энергоэффективность привлекает внимание инвесторов и деловых партнеров, благодаря чему можно развивать новые экономические связи и сотрудничество.

Настоящие требования по энергоэффективности жилых зданий, строений и сооружений сформулированы в статье 11 Федерального закона [1]. В обобщенном виде они включают [5, 8]:

- показатели, характеризующие удельную величину расхода энергетических ресурсов на объектах [6, 7];
- требования к инженерно-техническим решениям, влияющим на энергетическую эффективность [9].

Энергоэффективность достигается за счет внедрения более технологичных инженерно-технических коммунальных систем и высокого качества строительных матсриалов[5].

Существует десять классов энергоэффективности - от самого низкого E до наивысшего A++ (таблица 1). Согласно российскому законодательству классы энергоэффективности присваиваются многоквартирным домам начиная с 2014 года. При этом новостройкам определяется на основе проектной документации, анализ которой осуществляет Госстройнадзор. Дома, которые уже находятся в эксплуатации, класс присваивается по желанию жильцов, на основе изучения объекта Государственной жилищной инспекцией. В обоих случаях, объективные данные можно получить только после нескольких лет эксплуатации зданий, сравнивая реальное потребление энергоресурсов с нормативными показателями.

Таблица 1 – Классы энергоэффективности жилых домов.

Обозначение класса	Наименование класса	Величина отклонения расхода тепловой энергии на отопление и вентиляцию здания от нормируемого, %	Мероприятия
При проектировании и эксплуатации новых и реконструируемых зданий			
A++	Очень высокий	Ниже -60	Льгота по налогу на имущество на 3 года
A+	От -50 до -60 включительно		
A	От -40 до -50 включительно		
B+	Высокий	От -30 до -40 включительно	
Обозначение класса	Наименование класса	Величина отклонения расхода тепловой энергии на отопление и вентиляцию здания от нормируемого, %	Мероприятия
B	От -15 до -30 включительно		–
C+	Нормальный	От -5 до -15 включительно	
C	От +5 до -5 включительно		
C-	От +15 до +5 включительно		
При эксплуатации существующих зданий			
D	Пониженный	От +15,1 до +50 включительно	Реконструкция при соответствующем

			экономическом обосновании
E	Низкий	Более +50	Реконструкция при соответствующем экономическом обосновании, или снос

Дома, возведенные двадцать и более лет назад относятся к классу С. Еще более старые маркируются D и E, что говорит об отсутствии у них какой-либо энергетической эффективности. В принципе это объяснимо, так как до 2000-х годов энергосберегающие технологии не были распространены. Отсюда на этих объектах большие потери через наружные ограждающие конструкции, что приводит к высоким затратам на отопление[10].

Класс новостроек представлен классом от С до А+. Большинство зданий в сегменте «комфорт» строятся с присвоением класса В. Премиальная недвижимость - чаше всего с классом А. Согласно данным Центра энергосбережения (СПбБУ) наивысшие классы А+ и А++ говорят о том, что здание потребляет на 50-60% энергии меньше, чем к нему подведено [2].

Проблему постоянного роста жилищно-коммунальных тарифов может быть компенсирована в жилищном секторе разработкой энергоэффективных мероприятий в зданиях, подлежащих капитальному ремонту. До сих пор капитальный ремонт осуществлялся в отсутствии экономически и технически обоснованных нормативных требований к повышению энергетической эффективности. Более того, само производство работ по капитальному ремонту выведено из сферы ответственности органов строительного надзора.

Показатели энергоэффективности для новых зданий должны соответствовать в полной мере и для жилого строительства после проведенного капитального ремонта. Одним из основных критериев выполнения требований к энергетической эффективности объектов жилищного строительства после капитального ремонта должно являться выполнение нормативов по удельному энергопотреблению [3].

Поэлементные требования не первостепенны и контролируются только в исключительных случаях при отсутствии возможности реализации при капремонте необходимых технических решений.

Важно учитывать стоимость жизненного цикла технических решений по повышению энергоэффективности с учетом прогнозируемого повышения тарифов на энергоресурсы. Опыт показывает, что временной лаг составляет не менее 30 лет.

Нормативы энергоэффективности жилых домов зависят в том числе от отдельных инженерных систем. Это необходимо учитывать прежде всего, при проектировании или реконструкции данных систем.

Контроль за соблюдением гребований по энергоэффективности должен постоянно осуществляться в рамках системы мониторинга с возможностью корректировки управляющих воздействий.

На примере системы отопления рассмотрим требуемый уровень эффективного теплопотребления. который должен включать следующие элементы:

- системы автоматического регулирования и поддержание температурного напора во входной зоне зданий и сооружений;

- процессы регулирования теплопередачи на стояках и приборах отопления, с учетом температурного графика;
- автоматическое поддержание требуемого (расчетного) температурного напора теплоносителя на всех участкам системы отопления;
- оплату ресурсов по фактическому теплопотреблению.

Модернизация узла ввода систем теплопотребления здания жилого дома является одним из основных элементов по снижению тепловых потерь. Наиболее современным и эффективным решением является применение автоматизированного узла управления, который обеспечивает оптимальное теплопотребления здания в зависимости от температурного графика наружного воздуха, с требуемой эффективной циркуляции теплоносителя. Так в зависимости от состояний здания применение данного оборудование позволяет достигнуть экономического эффект от 12 до 30%.

Другим решением является распределение потока теплоносителя, позволяющее оптимизировать тепловую нагрузку на стояках вертикальных систем отопления Автоматические балансировочные клапана поддерживают изменения перепада давления в двухтрубных системах и поддерживают постоянный расход в однотрубных системах.

Результаты обследования типовых секционных зданий показал, что расход теплоносителя изменялся в пределах 30%. Установка балансировочных клапанов позволила снизить разброс расхода до 3-4%. Общее теплопотребление зданий снизилось до 12% за счет изменения настроек автоматики улов учета контролирующих температурный режим в наиболее удаленных стоках отопления, а также уменьшилось в помещениях из-за перегона на ближних стояках.

Вариантом снижения потерь для однотрубных систем отопления может стать применение терморегуляторов на стояках зданий, при совместной работе с балансировочными клапанами. Так возможно регулировать температуру теплоносителя на отдельных стояках путем закрытия термостатов, что сокращает избытки тепла в определенных помещениях, а не во всем здании.

Исследование результатов работы терморегуляторов на стояках однотрубных систем отопления показало сокращение расхода теплоносителя и повышение температуры теплоносителя в результате срабатывания термостатов на отдельных отопительных приборах. Температура воздуха при этом в контролируемом помещении остается постоянной.

Эффективное терморегулирование на стояках отопления зависит от величины неучтенных в проектных решениях избыточных тепловых поступлений, например от развитых поверхностей напева приборов отопления.

Управление энергосбережением организации ЖКХ также включает преобразование ее бизнес-модели. Бизнес-модель должна демонстрировать особенности организации бизнеса как системы, описывать взаимосвязь ее элементов, способы создания стоимости, получения прибыли и обеспечения конкурентного преимущества и должна состоять из взаимосвязанных компонентов, формирующих архитектуру эффективного энергосбережения в организации бизнеса [4].

Формализация такой бизнес-модели является основой для разработки комплекса мероприятий, составляющих программу энергосбережения и/или энергоаудита, которая является основным прикладным инструментом для решения главной задачи

энергосбережения-повышения энергоэффективности организации бизнеса. Перечень мероприятий программы энергосбережения может быть составлен в рамках каждого из внутренних факторов энергосбережения, поскольку они являются уровнями, на которые бизнес-организация может непосредственно влиять для повышения энергоэффективности своей деятельности и, как следствие, получения дополнительных конкурентных преимуществ.

Основными внутренними факторами энергосбережения в хозяйственной организации, на мой взгляд, являются следующие: организационно-управленческая структура, профессиональная и психологическая подготовка работников в области энергосбережения, производственная структура, условия и источники энергии, способ производства, структура расхода продукции, характеристики готовой продукции, а также особенности эксплуатации оборудования. В соответствии с этим подходом все мероприятия программы энергосбережения в хозяйственной организации предлагается рассматривать в рамках двух групп: технических и организационных. По глубине изменений и величине затрат, необходимых для их реализации, эти мероприятия могут быть базовыми (малозатратными), углубленными и глубокими, а по характеру планируемых изменений их можно отнести к конструктивным, технологическим и конструктивно-технологическим [4].

Следует отметить, что даже те хозяйственные организации, деятельность которых связана с высоким энергопотреблением, должны не только осуществлять технические мероприятия, направленные на снижение энергоемкости производства, но и уделять пристальное внимание организационным мероприятиям по энергосбережению. Организационные мероприятия обеспечивают совершенствование энергосберегающих процессов, их адаптацию к динамичной внешней среде и позволяют организации бизнеса гораздо эффективнее использовать потенциал технических мероприятий.

Таким образом, можно констатировать, что управление энергосбережением большинства отечественных хозяйственных организаций в системе ЖКХ характеризуется фрагментарностью. В последние годы значительно возрос уровень заинтересованности собственников бизнес-организаций в повышении энергоэффективности своих предприятий, внедрении в практику энергоаудита и политики энергосбережения. Однако ситуация характеризуется наличием барьеров для инвестирования в энергоэффективность, а также необходимостью совершенствования существующих бизнес-моделей компаний, функционирующих в современной системе ЖКХ.

Список литературы

1. Крючков Д.Г. Повышение энергоэффективности в жилищнокоммунальном хозяйстве: тенденции и проблемы. / Д.Г. Крючков, В.А. Зайцев // Энергосбережение. Энергетика. Энергоаудит – 2019. № 11. 22-26 с.
2. Иванова Е.В. Меры по снижению потерь энергии в системах жилищно-коммунального хозяйства. / Е.В. Иванова, А.Н. Петров // Вестник инженерной академии – 2020. № 3. 45-50 с.
3. Смирнов Г.П. Проблемы и перспективы энергосбережения в жилищно-коммунальном комплексе России. / Г.П. Смирнов, В.М. Козлов // Энергетика и ресурсосбережение – 2018. № 4. 12-18 с.

4. Горбунов А.И. Энергоэффективные технологии в системе жилищно-коммунального обслуживания. / А.И. Горбунов, О.С. Николаева // Экология и промышленность России – 2021. № 5. 15-20 с.
5. Павлов Д.С. Оценка эффективности мероприятий по повышению энергоэффективности в жилищно-коммунальном секторе. / Д.С. Павлов, В.В. Андреев // Энергетика и экология – 2019. № 2. 32- 37 с.
6. Морозова, И. В., & Максимов, В. Н. (2019). Оценка энергоэффективности в ЖКХ: теория и практика. Вестник Казанского государственного архитектурно-строительного университета, (4), 242-253.
7. Литвинов, А. (2018). Энергоэффективность в жилищно-коммунальном хозяйстве. Вестник науки и образования, (3), 38-43.
8. Кравченко, В. В., Осипенко, В. В., & Решетников, Ф. А. (2017). Повышение энергоэффективности жилищно-коммунального хозяйства. Вестник Витебского государственного технологического университета, (6), 123-129.
9. Саркисов С.В., Путилин П.А., Ивановский В.С., Игнатчик В.С. Методика оптимизации систем водоснабжения // Труды Военно-космической академии им. А.Ф. Можайского. - 2015. №649. С. 181-187.
10. Кармазинов Ф.В., Игнатчик В.С., Саркисов С.В. и др. Методика оптимизации зональных систем водоснабжения // Водоснабжение и санитарная техника. - 2016. №2. С. 64-70.

References

1. Kryuchkov D.G. Improving energy efficiency in housing and communal services: trends and problems. / D.G. Kryuchkov, V.A. Zaitsev // Energy saving. Energy. Energy Audit – 2019. No. 11. 22-26 p.
2. Ivanova E.V. Measures to reduce energy losses in housing and communal services systems. / E.V. Ivanova, A.N. Petrov // Bulletin of the Engineering Academy - 2020. No. 3. 45-50 p.
3. Smirnov G.P. Problems and prospects of energy saving in the housing and communal complex of Russia. / G.P. Smirnov, V.M. Kozlov // Energetika i resursosberezhenie – 2018. No. 4. 12-18 p.
4. Gorbunov A.I. Energy-efficient technologies in the system of housing and communal services. / A.I. Gorbunov, O.S. Nikolaeva // Ecology and industry of Russia – 2021. No. 5. 15-20 p.
5. Pavlov D.S. Evaluation of the effectiveness of measures to improve energy efficiency in the housing and communal sector. / D.S. Pavlov, V.V. Andreev // Energetika i ekologiya – 2019. No. 2. 32- 37 p.
6. Morozova, I. V., & Maksimov, V. N. (2019). Energy efficiency assessment in housing and communal services: theory and practice. Bulletin of the Kazan State University of Architecture and Civil Engineering, (4), 242-253.
7. Litvinov, A. (2018). Energy efficiency in housing and communal services. Bulletin of Science and Education, (3), 38-43.
8. Kravchenko, V. V., Osipenko, V. V., & Reshetnikov, F. A. (2017). Improving the energy efficiency of housing and communal services. Bulletin of the Vitebsk State Technological University, (6), 123-129.

9. Sarkisov S.V., Putilin P.A., Ivanovsky V.S., Ignatchik V.S. Methods of optimization of water supply systems // Proceedings of the Military Space Academy named after A.F. Mozhaisky. - 2015. No.649. pp. 181-187.
10. Karmazinov F.V., Ignatchik V.S., Sarkisov S.V. and others. Methodology of optimization of zonal water supply systems // Water supply and sanitary equipment. - 2016. No. 2. pp. 64-70.

Кутмухамедова А.А. Процесс проектирования инженерных сетей// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 5(43) с. 134–142

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 624

ПРОЦЕСС ПРОЕКТИРОВАНИЯ ИНЖЕНЕРНЫХ СЕТЕЙ

Кутмухамедова А.А.
ФГАОУ ВО «УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИИ Б.Н. ЕЛЬЦИНА», Екатеринбург, Россия, (620002, Свердловская область, город Екатеринбург, ул. Мира, д. 19), e-mail: ainura-01@mail.ru

Статья посвящена проектированию инженерных систем зданий. Рассматриваются этапы проектирования начиная с отопления и заканчивая системами безопасности и телекоммуникаций. Особое внимание уделяется многоэтапности процесса проектирования, куда входит анализ потребностей, разработка технических заданий, детальное проектирование и экспертиза. Подчеркивается значимость каждой системы для создания функционального и безопасного пространства.

Ключевые слова**:** Проектирование инженерных систем, внутренние инженерные системы, отопительная система, системы безопасности, телекоммуникации, энергоэффективность.

THE PROCESS OF DESIGNING ENGINEERING NETWORKS

Kutmukhamedova A.A.
URAL FEDERAL UNIVERSITY NAMED AFTER THE FIRST PRESIDENT OF RUSSIA B.N. YELTSIN, Yekaterinburg, Russia, (19 Mira st., Yekaterinburg, Sverdlovsk Oblast, 620002), e-mail: ainura-01@mail.ru

The article is devoted to the design of engineering systems of buildings. The stages of design are considered, starting with heating and ending with security and telecommunications systems. Special attention is paid to the multi-stage design process, which includes needs analysis, development of technical specifications, detailed design and expertise. The importance of each system for creating a functional and safe space is emphasized.

Keywords: Engineering systems design, internal engineering systems, heating system, security systems, telecommunications, energy efficiency.

Любое строительство зданий и сооружений начинается с проектирования. Проект является детальным описанием будущего объекта со всеми необходимыми расчетами и дополнениями. Сегодня без проектирования инженерных сетей невозможно представить ни одно современное здание, так как процесс является очень важной частью общего проекта, поэтому допущенные при проектировании ошибки могут обойдись для заказчика не только очень дорого, но и привести к авариям различного масштаба.

Сегодня инженерные сети делятся на внутренние и внешние. К проектированию внутренних сетей относятся:

- отопительная система, водоснабжения и канализация с очисткой стоков.
- вентиляционная система здания и кондиционирование его помещений.
- электроснабжение и осветительная система.

- слаботочные системы – сигнализация, видеонаблюдение, диспетчеризация инженерных системы, системы «Умный дом» и так далее.

Для строящихся крупных предприятий, к примеру, сложность проектирования этих систем заключается в рациональном использовании внутреннего пространства, которое должно приносить собственнику максимальную прибыль и при этом отвечать всем требованиям безопасности.

Процесс проектирования внутренних инженерных сетей здания основывается на следующих этапах:

1. Сбор информации об объекте проектирования – анализ информации, разработка предварительной концепции.

2. Разработка эскизного проекта и технико-экономического предложения – это визуальное оформление на предоставленных Заказчиком планах объекта строительства основной идеи (концепции) функционирования и расположения основных элементов инженерной системы.

3. Разработка технического задания (ТЗ) на создание инженерной системы – составление перечня требований, условий, целей, задач, которые должны быть реализованы в проектной документации, поставленных от лица Заказчика и оформленных документально.

4. Разработка проектной документации и коммерческого предложения – оформляются технические решения для производства монтажных работ по инженерной системе без их деталировки и спецификации.

5. Разработка рабочей документации на инженерные системы – разрабатывается необходимый пакет документов для производства работ по созданию внутренней инженерной системы. Пакет документов включает в себя детальные планы, спецификацию инженерного оборудования с их характеристиками, а также спецификацию на используемые материалы.

Начинается процесс проектирования с разработки отопительной системы, поскольку в условиях климата России затраты на отопление являются одной из самых значительных статей расходов в строительстве. В секторе промышленного строительства эта задача стоит особенно остро из-за больших площадей объектов и высокой энергоемкости используемого оборудования, что делает невозможным применение стандартных решений.

Особое внимание в процессе проектирования уделяется обеспечению высокой надежности отопительной системы, поскольку любые сбои или аварии могут привести к серьезным последствиям: повреждению оборудования, риску для здоровья персонала и возможность длительных простоев производства. Для минимизации таких рисков предусматривается внедрение систем полной или частичной автоматизации управления отопительной системой. Благодаря этому можно оптимизировать ее работу и обеспечить эффективное реагирование на возникающие проблемы. Проектирование производится в несколько этапов [4, с. 37]:

Первый этап – предварительный анализ и сбор данных:

- изучение климатических условий региона для определения оптимальных параметров отопительной системы;
- анализ специфики объекта строительства, включая площадь, объем помещений, предназначение здания и требования к температурному режиму;

- сбор исходных данных о доступных энергоресурсах, возможностях подключения к внешним сетям и ограничениях, наложенных законодательством и нормативами.

Второй этап – разработка предварительной концепции:

- определение основных технических решений, включая выбор типа отопительной системы (централизованная, автономная), видов топлива, принципов управления и автоматизации;
- разработка концептуальных схем распределения тепловой энергии по объекту.

Третий этап – технико-экономическое обоснование:

- расчет потребности в тепловой энергии исходя из теплопотерь здания и необходимых параметров микроклимата;
- оценка экономической эффективности предложенных решений, включая анализ затрат на установку и эксплуатацию системы, сроки окупаемости.

Четвертый этап – разработка технического задания:

- формулирование технических требований к отопительной системе, включая параметры температуры, мощности, надежности и безопасности;
- уточнение условий эксплуатации и требований к системе управления и автоматизации.

Пятый этап – проектирование системы:

- детальное проектирование всех элементов системы, включая расчеты мощности, выбор оборудования, проектирование маршрутов трубопроводов и расположение теплогенерирующего оборудования;
- разработка схем управления и автоматизации, обеспечивающих оптимальный режим работы и возможность оперативного реагирования на изменение условий;
- подготовка проектной документации, включающей все технические решения, схемы и расчеты;
- создание рабочей документации, необходимой для монтажа, пусконаладочных работ и последующей эксплуатации системы.

Шестой этап – проведение экспертизы проекта на соответствие нормативам безопасности, экологии и энергоэффективности.

После разработки отопительной системы важнейшим этапом проектирования внутренних инженерных систем является создание систем водоснабжения и канализации. Одним из важнейших элементов этого этапа –проектирование очистных сооружений. Если речь идет о промышленных объектах, то необходимы очистные сооружения, которые способны обеспечивать высокую степень очистки сточных вод при минимальном расходе электроэнергии. Их конструкция должна быть направлена на оптимизацию производственных процессов, увеличение их производительности при соблюдении всех норм безопасности и надежности [1, с. 103].

В проекте также должна быть рассмотрена разработка водозаборного узла и станции подготовки питьевой воды, обеспечивающих соответствие санитарным и гигиеническим нормам. В условиях повышенных требований к экологической безопасности и рациональному использованию водных ресурсов для промышленных объектов может потребоваться реализация систем замкнутого водооборота, что позволяет значительно снизить потребление природных вод и минимизировать объемы сточных вод.

Особое внимание в процессе проектирования уделяется взаимодействие систем водоснабжения, отопления и канализации. Интеграция данных систем позволяет достигать высокой эффективности и экономии ресурсов за счет взаимодействия компонентов, например, сегодня активно практикуется использование отработанной тепловой энергии для подогрева воды. Этот этап требует тщательного планирования и координации на всех шагах проектирования, чтобы минимизировать риски возможных перекрестных помех, обеспечить эргономику расположения элементов и избежать дополнительных финансовых затрат на последующую корректировку проекта [2, с. 33].

В проектирование водоснабжения входят следующие этапы. Первый этап – анализ и планирование:

- изучение особенностей объекта для определения потребностей в водоснабжении и канализации;
- оценка исходных условий (анализ местных водных ресурсов, существующих систем и экологических требований);
- планирование очистных сооружений с учетом необходимой степени очистки и минимизации энергопотребления.

Второй этап – разработка концепции:

- выбор технологий очистки сточных вод, определение их расположения и масштабов в соответствии с производственными и экологическими требованиями.
- проектирование водозаборного узла и станции подготовки питьевой воды, обеспечение их соответствия санитарным нормам.
- разработка систем замкнутого водооборота для минимизации потребления воды и объемов сточных вод.

Третий этап – технико-экономическое обоснование:

- расчеты эффективности и экономии от внедрения предложенных систем и технологий;
- оценка стоимости реализации проекта, включая строительство очистных сооружений, водозаборных узлов и систем подготовки питьевой воды.

Четвертый этап – разработка технического задания:

- формулирование требований к системам водоснабжения и канализации, учитывая их взаимодействие с отопительной системой;
- уточнение параметров для системы управления и автоматизации, обеспечивающей эффективную и экономичную эксплуатацию.

Пятый этап – детальное проектирование:

- разработка подробных схем и чертежей, включая расположение труб, очистных сооружений, водозаборных узлов и других элементов систем;
- выбор оборудования и материалов, оптимально подходящих для заданных условий и требований.

Шестой этап – разработка проектной и рабочей документации:

- подготовка документации, описывающей все аспекты систем водоснабжения и канализации, включая технологические процессы очистки и подготовки воды;
- создание инструкций для строительства, монтажа, пусконаладочных работ и эксплуатации систем.

Ну и, наконец, последний этап – экспертиза и согласование проекта на соответствие нормам и стандартам безопасности, экологии и санитарии.

На третьем месте по значимости в процессе проектирования современных инженерных сетей находятся системы вентиляции и кондиционирования. Растущие требования к качеству воздуха, температурному режиму и влажности в помещениях, обусловленные как развитием новых производственных технологий, так и появлением высокотехнологичного оборудования, делают эти системы неотъемлемым элементом современных зданий.

Разработка эффективных систем вентиляции и кондиционирования требует комплексного подхода, который будет учитывать специфику использования здания, а также необходимость обеспечения оптимальных условий для комфорта людей и бесперебойной работы оборудования. Если речь идет о промышленных помещениях, то важно предусмотреть системы, способные обеспечивать стабильную температуру и влажность, необходимые для производственных процессов, а также отвод вредных выбросов.

Внедрение систем принудительной приточно-вытяжной вентиляции и кондиционирования в жилых и общественных зданиях стало стандартом, который необходим для комфортного проживания и пребывания людей. Достичь высокой эффективности и экономии энергоресурсов также позволяет интеграция с системами холодоснабжения, где температура в различных зонах здания может регулироваться индивидуально с помощью холодильных машин.

При проектировании систем вентиляции и кондиционирования особое внимание необходимо уделить не только техническим характеристикам оборудования, но и его энергоэффективности. Применение современных энергосберегающих технологий, например, рекуперации тепла, значительно позволит снизить энергопотребление при обеспечении необходимого микроклимата в помещениях. Это возможно благодаря использованию теплообменников, которые возвращают часть тепла или холода из вытяжного воздуха обратно в систему, сокращая тем самым потребление энергии на подогрев или охлаждение приточного воздуха.

Необходимо рассмотреть рассмотрим ключевые этапы этого процесса:

Первый этап – анализ потребностей и планирование:

- определение требований к качеству воздуха, температуре и влажности в зависимости от назначения помещений, учитывая как комфорт людей, так и требования к работе оборудования;
- изучение особенностей здания, его архитектурных и конструктивных особенностей для определения возможных вариантов систем вентиляции и кондиционирования.

Второй этап – разработка концепции системы:

- выбор типа системы вентиляции (естественная, принудительная приточно-вытяжная вентиляция, механическая вентиляция и т.д.) и системы кондиционирования воздуха, а также определение потребности в системах холодоснабжения;
- разработка предварительных схем расположения оборудования и каналов вентиляции с учетом архитектурных особенностей здания и требований к эффективности и экономии энергии.

Третий этап – технико-экономическое обоснование:

- расчет необходимой мощности оборудования и объема воздухообмена для обеспечения оптимального микроклимата;
- оценка экономической эффективности предлагаемых решений, включая анализ стоимости оборудования, установки и эксплуатации, а также расчет сроков окупаемости инвестиций.

Четвертый этап – разработка технического задания:

- формулирование технических требований к системам вентиляции и кондиционирования (параметры качества воздуха, температурные и влажностные режимы);
- определение требований к энергоэффективности и экологическим характеристикам системы.

Пятый этап – проектирование:

- подробное проектирование систем, включая разработку технических решений, выбор оборудования, расчет воздуховодов и каналов, а также систем управления и автоматизации;
- интеграция системы с другими инженерными системами здания, такими как отопление и водоснабжение, для обеспечения эффективного взаимодействия и оптимизации работы.

Этап шестой – разработка проектной и рабочей документации: создание полного пакета проектной документации, куда входят чертежи, схемы расположения оборудования и каналов, а также спецификации и технические условия на установку и эксплуатацию.

На седьмом этапе происходит проведение экспертизы проекта на соответствие нормам и стандартам, включая требования пожарной безопасности, санитарно-эпидемиологические нормы и стандарты энергоэффективности.

После чего производится проектирование электричества, без которого невозможно нормальное функционирование систем отопления, водоснабжения и водоотведения, а также вентиляции, не говоря уж об оборудовании. Электросети должны соответствовать следующим требованиям [3, с. 45]:

- бесперебойная и стабильная подача электроэнергии;
- безопасность сетей для пользователей;
- соответствие электросистем всем действующим нормам и стандартам;
- безопасность электросетей при их регулярном обслуживании.

Проектировщики также должны предусмотреть возможности увеличения нагрузки электросистемы, ее автоматизацию и минимизацию расходов на эксплуатацию сетей. Проектирование электросети также подразделяется на несколько этапов:

Первый этап – анализ потребностей и исходных данных:

- оценка общей потребности в электроэнергии здания, исходя из предполагаемых нагрузок всех инженерных систем и оборудования;
- изучение условий подключения к внешним источникам питания и существующей инфраструктуры электроснабжения.

Второй этап – разработка концепции системы электроснабжения:

- выбор системы электроснабжения (централизованное, резервное, автономное) в зависимости от требований к надежности и безопасности;

- планирование распределительной сети внутри здания, включая определение мест расположения щитов, кабельных трасс и оборудования.

Третий этап – технико-экономическое обоснование:

- расчет стоимости реализации системы электроснабжения, включая оборудование, материалы и работу;
- анализ возможностей для оптимизации расходов на электроэнергию, в том числе через использование энергосберегающих технологий.

Четвертый этап – разработка технического задания:

- формулирование требований к электроснабжению, учитывая все аспекты безопасности, надежности и экономичности;
- учет возможного будущего расширения системы и увеличения нагрузок без существенных изменений инфраструктуры.

Пятый этап – проектирование:

- разработка схем электроснабжения, включая выбор оборудования (кабели, автоматы, УЗО, щиты и т.д.);
- расчет и проектирование системы автоматизации управления электроснабжением для повышения его эффективности и безопасности.

Шестой этап – разработка проектной и рабочей документации:

- создание полного комплекта документации, включающего все необходимые чертежи, схемы и спецификации;
- подготовка технических условий для установки, пусконаладочных работ и дальнейшей эксплуатации системы.

На седьмом этапе проводится экспертиза проекта на соответствие действующим нормам и стандартам, в том числе требованиям пожарной безопасности и электробезопасности.

Следующим шагом является разработка системы освещения. Сюда сходит подбор осветительных приборов и расчет освещенности для создания комфортных условий для проживания и работы, а также энергоэффективности и соответствия нормативам по освещенности. Важно уделить внимание проектированию противопожарных систем: систем оповещения, пожаротушения и эвакуации. Они предназначены для минимизации рисков и обеспечения безопасности людей и имущества в случае пожара.

Следующим этапом является разработка систем телекоммуникаций, куда входит интернет-инфраструктура, системы видеонаблюдения, связи и данных. Они играют ключевую роль в обеспечении бесперебойной коммуникации и безопасности зданий.

Для того, чтобы упросить процесс проектирования можно использовать BIM (Building Information Modeling) – это современная технология и процесс, который позволяет архитекторам, инженерам, строителям и владельцам проектов совместно проектировать, визуализировать, симулировать и управлять информацией о строительстве и эксплуатации объектов на протяжении всего их жизненного цикла, от концепции до сноса.

Применение BIM в процессе проектирования инженерных систем зданий значительно повышает его эффективность, позволяя достичь следующих преимуществ:

1. Улучшение визуализации проекта. BIM предоставляет трехмерное представление строения, благодаря чему можно лучше понять проект в целом и оценить влияние отдельных элементов системы друг на друга и на общую функциональность здания.

2. Координация и интеграция. Технология BIM позволяет синхронизировать работу различных специалистов, вовлеченных в проект, обеспечивая высокую степень интеграции и координации всех инженерных систем, что снижает вероятность ошибок и несоответствий в проекте.

3. Оптимизация процессов. Благодаря BIM можно проводить анализ эффективности проектируемых систем, оптимизировать их работу, выбирать наиболее подходящее оборудование и материалы, а также предсказывать и управлять затратами на строительство и эксплуатацию объекта.

4. Поиск конфликтов. Главным преимуществ BIM является возможность автоматического обнаружения конфликтов между различными системами (например, между вентиляционными каналами и несущими конструкциями) еще на стадии проектирования, что позволяет избегать дорогостоящих изменений в процессе строительства.

5. Поддержка устойчивого развития. При помощи данного инструмента, можно разрабатывать более энергоэффективные и экологически устойчивые решения за счет анализа энергопотребления и выбора оптимальных технологий.

6. Управление данными в реальном времени. Благодаря BIM обеспечивается доступ к актуальной информации о проекте для всех участников на всех этапах его реализации, облегчая процесс внесения изменений, обновления документации и управления строительством.

Таким образом, проектирование внутренних инженерных систем здания – это комплексный процесс, который требует междисциплинарного подхода и внимания к деталям на каждом этапе. От систем отопления, водоснабжения и канализации до систем электроснабжения, освещения, противопожарной безопасности и телекоммуникаций – каждый элемент важен для создания функционального, комфортного и безопасного пространства.

Список литературы

1. Бутко Д.А. Проектирование сооружений водопровода и канализации/Д.А.Бутко, В.А.Лысов, Л.И.Нечаев//Строительство и архитектура–2015: материалы международной научно-практической конференции, Ростов-на-Дону, 26–27 ноября 2015 года/ФГБОУ ВПО «Ростовский гос.строит.университет», Союз строителей южного федерального округа, Ассоциация строителей Дона. Том 2. – Ростов-на-Дону: Редакционно-издательский центр РГСУ, 2015. – С. 103-105.
2. Квасов, И. С. Проектирование распределительных систем отопления/ И. С. Квасов, М. Я. Панов // Программные средства для информатизационных технологий, используемых во ВГАСУ: Аннотированный каталог. – 2-е издание, дополненное. – Воронеж: Воронежских государственный архитектурно-строительный университет, 2002. – С. 33.
3. Проектирование и электрическая часть // Светотехника. – 2006. – № S5. – С. 43-50.
4. Шапенкова, А. В. Методы и подходы к проектированию эффективных систем отопления и вентиляции в производственных помещениях / А. В. Шапенкова // Молодой ученый. – 2023. – № 47(494). – С. 37-40.

References

1. Butko, D. A. Design of water supply and sewerage structures / D. A. Butko, V. A. Lysov, L. I. Nechaeva // Construction and Architecture 2015 : materials of the International scientific and Practical conference, Rostov-on-Don, November 26-27, 2015 / Rostov State University of Civil Engineering, Union of Builders of the Southern Federal District, Association of Builders of the Don. Volume 2. – Rostov-on-Don: Editorial and Publishing Center of the Russian State University of Economics, 2015. – pp. 103-105.
2. Kvasov, I. S. Design of distribution heating systems/ I. S. Kvasov, M. Ya. Panov // Software tools for informatization technologies used in VGASU: An annotated catalog. – 2nd edition, supplemented. Voronezh: Voronezh State University of Architecture and Civil Engineering, 2002. - p. 33.3.
3. Design and electrical part // Lighting Engineering. - 2006. – No. S5. – pp. 43-50.
4. Shapenkova, A.V. Methods and approaches to the design of efficient heating and ventilation systems in industrial premises / A.V. Shapenkova // Young Scientist. – 2023. – № 47(494). – pp. 37-40.

Червяков М.А. Организационно-технологические решения при строительстве школ с применением энергоэффективных технологий// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 143–147

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 69

ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ ПРИ СТРОИТЕЛЬСТВЕ ШКОЛ С ПРИМЕНЕНИЕМ ЭНЕРГОЭФФЕКТИВНЫХ ТЕХНОЛОГИЙ

Червяков М.А.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ", Санкт-Петербург, Россия (190005, город Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: 3amestermaks2000@gmail.com

На территории России стала активно реализовываться программа внедрения энергосберегающих технологий в процессе строительства зданий различного предназначения, в том числе и образовательной направленности. В данной работе анализируется текущее состояние по внедрению программ энергосбережения в России при строительстве школ. Представлен обзор двух школьных зданий и их текущего состояния. Кроме того, следует отметить, что применение энергосберегающих технологий в период строительства школ положительным образом сказывается и на экономических затратах, были даны рекомендации для повышения энергетической эффективности этих зданий и проведен расчет, доказывающий экономическую эффективность данных предложений.

Ключевые слова: Энергоэффективный, энергосбережение, школа, теплоэнергия, здание.

ORGANIZATIONAL AND TECHNOLOGICAL SOLUTIONS FOR THE CONSTRUCTION OF SCHOOLS USING ENERGY-EFFICIENT TECHNOLOGIES

Chervyakov M.A.
ST. PETERSBURG STATE UNIVERSITY OF ARCHITECTURE AND CIVIL ENGINEERING, St. Petersburg, Russia (190005, St. Petersburg, 2nd Krasnoarmeyskaya str., 4), e-mail: 3amestermaks2000@gmail.com

A program for the introduction of energy-saving technologies in the construction of buildings of various purposes, including educational orientation, has been actively implemented in Russia. This paper analyzes the current state of implementation of energy saving programs in Russia during the construction of schools. An overview of two school buildings and their current condition is presented. In addition, it should be noted that the use of energy-saving technologies during the construction of schools has a positive effect on economic costs, recommendations were made to increase the energy efficiency of these buildings and a calculation was carried out proving the economic effectiveness of these proposals.

Keywords: Energy efficient, energy saving, school, heat energy, building.

Как правило, под политикой энергосбережения подразумеваются определенного рода запреты и ограничения, направленные на рациональное использование энергоресурсов. Благодаря данному ответственному отношению образовательные учреждения приобретут возможность экономить на закупке тепла и электричества. Тема данной статьи является весьма

актуальной не только с точки зрения бережного отношения к экологии, но и с позиции улучшения благосостояния общества [1].

В энергетическом плане Российской Федерации на временной промежуток до 2030 г. указан факт, заключающийся в большой проблеме неосуществлённости потенциала управленческого и технологического энергосбережения, насчитывающий около 40 % общего объема внутреннего потребления. Именно поэтому в седьмой статье Федерального закона «Об энергосбережении и повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации» обозначено то, что к полномочиям госорганов субъектов Российской Федерации в сфере энергосбережения и увеличения энергетической результативности относится осуществление региональных программ данной тематики [2].

В качестве первого реализованного проекта выступает государственная общеобразовательная средняя школа №2 Самарской области.

Электроснабжение строения реализовывается с помощью трансформатора до вводно-распределительного устройства.

Теплоснабжение школы реализуется от котельной ЖКХ. Температурный график источника составляет (95-70) ^{0}С. Подключение отопления осуществляется через двухтрубную закрытую систему, для горячего водоснабжения используются электрические водонагреватели. Разводка труб отопления горизонтальная. В системе отопления используются чугунные радиаторы и стальные регистры.

Система теплоснабжения находится в удовлетворительном состоянии. Радиаторы отопления имеют сниженные характеристики теплоотдачи из-за отложений во внутреннем объеме. Для улучшения показателей в помещении рекомендуется устанавливать за радиаторами теплоотражатели.

Работающий радиатор усиленно прогревает участок стены, который располагается за ним. Благодаря этому температура данного участка гораздо больше по сравнению с остальной областью. Следовательно, вместо того, чтобы задействовать все тепло для обогрева внутреннего объема помещения, прибор усиленно тратит энергию на нагрев материалов наружных стен здания. Необходимость снижения теплопотерь, в таких ситуациях целесообразно установить теплоотражающий экран, чтобы изолировать участок стены за обогревателем. Для изготовления таких экранов используются материалы с низкой теплопроводностью (около 0,05 Вт/м*С).

Предполагаемые затраты:

Рекомендуется установка 8-ми миллиметровой теплоотражающей пленки, которая ровна площади стены, расположенной за радиатором - 179,85 кв.м., в среднем около 200 рублей за квадратный метр [8].

В данной системе теплоснабжения в среднем 35% общей тепловой энергии передается излучением для обогрева, из которых около 40% используется для обогрева стен. Исключение потерь от обогрева конструкций за радиаторами излучением позволяет сэкономить на использовании тепловой энергии. На основе статистических данных по этому показателю было установлено, что в среднем температура внутри здания повысится на 1 градус Цельсия. Исходя из этого, рассчитывается количество тепла, необходимое данному зданию для повышения температуры в помещениях на 1,5 градуса. Таким образом, получается

натуральный показатель экономической выгоды. [4]. Чтобы физически рассчитать годовую экономию, используйте следующую формулу:

$$\delta = \frac{\alpha \bullet (\ q_b + q_o\ ) \bullet V \bullet (t_2 - t_1\ ) \bullet T_0}{1000000}, \quad (1)$$

где а – это коэффициент, который учитывает изменение удельной тепловой характеристики здания и зависит от климатических условий (температуры наружного воздуха) - принимаем равным 1; $q_в$ - удельная тепловая характеристика здания для вентиляции, ккал/(м3*ч*С); V- объем здания наружный, м3; t_2 - температура внутри здания до реализации мероприятия, C^0; t_1 - температура в помещениях после реализации мероприятия, C^0; T_0- продолжительность отопительного периода, ч.

В результате расчета, что экономия составляет 13,26 Гкал. При тарифе равном 1294 рублей/Гкал экономия составит 17,159 тыс.рублей [7]. Срок окупаемости составит 2,10 года.

В качестве второго реализованного объекта выступает средняя общеобразовательная школа №2, которая находится в Киришах.

В школьных зданиях циркуляция воздуха должна быть не реже одного раза в час в соответствии с гигиеническими нормами. Это обеспечивается системой вентиляции. Выполним расчет теплопотерь в школьном здании, если температура внутри +20°С, а за окном -20°С.. Стены кирпичные, толщиной 0,75 м.

Мощность теплопотерь оценивается по следующему выражению:

$$W = \frac{S \bullet c \bullet (T_{вн} - T_{си})}{d}, Вт, \quad (2)$$

где d – толщина стен; S – общая площадь стен, через которую теряется тепло; с – коэффициент теплопроводности кирпича.

В результате расчета получаем, что мощность тепловых потерь стенами составляет 192296,53 Вт, следовательно, 1м^2 стены теряет 37,3 Вт [5].

Общий объем воздуха в школе V равен примерно 22000 м^3 [8].

V = 22000м^3 воздуха поступает в здание из вне (расход 2 м^3 /с). Этот воздух нагревается и поступает в вентиляционные трубы. Воздух нагревается при постоянном давлении, поэтому мощность теплопотерь при вентиляции вычислим по формуле:

$$W = \frac{pw}{\mu(T_{ав} - T_{си})} \bullet \frac{7}{2} \bullet \frac{R}{t} Вт, \quad (3)$$

где t — время, R — универсальная газовая постоянная, μ — молярная масса воздуха, p — плотность воздуха.

Мощность тепловых потерь от вентиляции составила 316257,56 Вт, а суммарная мощность – 508554,1 Вт.

В школе обучается 845 учеников, что означает теплопотери в 601,8 Вт на ученика. При этом, один человек в среднем вырабатывает около 100 Вт тепловой мощности. Это означает, что покрывается только 16,6% требуемой потребности в тепле. [6].

Посредством анализа строительства и реализации школ с применением энергоэффективных технологий были выявлены следующие общие недостатки и сформулированы следующие рекомендации:

1. Надо выполнить утепление ограждающих конструкций.

2. Так как кровельное покрытие является основным тепловым барьером, необходимо его обновить: добавить слой пароизоляционного материала, чтобы предотвратить попадание влаги в слой тепловой утеплителя; уложить два слоя теплоизоляции.
3. Перекрытия не утеплены. Проложить слой теплоизоляции для нижнего этажа.
4. Установить систему погодного регулирования, способную количественно регулировать подачу тепла в систему отопления путем задания необходимой температуры теплоносителя с помощью электронного регулятора в соответствии с заданным температурным графиком. Замена отопительного оборудования.

Список литературы

1. Гринчук, И.С. Зеленое строительство, как один из важнейших аспектов устойчивого развития/ И.С. Гринчук, Н.Г. Синяк // Труды БГТУ. №7. Экономика и управление. URL: https://e.lanbook.com/journal/issue/294335 (дата обращения: 11.03.2024).
2. Молодые ученые – развитию Национальной технологической инициативы. 24 – 27 апреля 2023 года: материалы конференции. Иваново: ИВГПУ, 2023. 1110 с. ISBN 978-5-88954-511-8. URL: https://e.lanbook.com/book/338105 (дата обращения: 12.03.2024).
3. Отчет об энергетическом обследовании ГБОУ СОШ №2.
4. Порфирьев, Д. Н. Экономика организации: учебное пособие / Д. Н. Порфирьев. Пенза: ПГАУ, 2022. 193 с.
5. Строительная физика: методические указания / составитель И. А. Обухова; под редакцией Г. И. Полищук. Санкт-Петербург: СПбГЛТ, 2019. 44 с.
6. Ушаков, В. Я. Потенциал энергосбережения и его реализация в секторах конечного потребления энергии: учебное пособие / В. Я. Ушаков, Н. Н. Харлов, П. С. Чубик. Томск: ТПУ, 2015. 388 с. URL: https://e.lanbook.com/book/82837 (дата обращения: 15.02.2024).
7. Экономика и финансы образования (учебное пособие) / С.А. Беляков, В.А. Дмитриева, в.В. Дудников и др.; Под. ред. С.А. Белякова, М.М. Мусарского. М.: Издательство МГОУ, 2002. 280 с.
8. Энергосбережение в теплоэнергетике и теплотехнологиях: учебник / А. Б. Гаряев, И. В. Яковлев, А. В. Клименко [и др.]. URL: https://e.lanbook.com/book/362507 (дата обращения: 16.03.2024).

References

1. Grinchuk, I.S. Green construction as one of the most important aspects of sustainable development/ I.S. Grinchuk, N.G. Sinyak // Trude BGTU [Proceedings of BSTU]. No.7.Economics and Management URL: e.lanbook.com/journal/issue/294335
2. Young scientists – development of the National Technology Initiative (SEARCH – 2023). April 24 – 27, 2023: conference proceedings. Ivanovo: IVSPU, 2023. p. 1110. URL: e.lanbook.com/book/338105
3. Report on the energy survey of GBOU Secondary School No. 2.
4. Porfiriev, D. N. Economics of organization / D. N. Porfiriev. Penza: PGAU, 2022. p. 193.
5. Construction physics: methodological guidelines / compiled by I. A. Obukhov; edited by G. I. Polishchuk. St. Petersburg: SPbGLT, 2019. p. 44.

6. Ushakov, V. Ya. The potential of energy saving and its implementation in the sectors of final energy consumption / V. Ya. Ushakov, N. N. Kharlov, P. S. Chubik. Tomsk: TPU, 2015. p. 388.
7. Economics and finance of education/ S.A. Belyakov, V.A. Dmitrieva, V.V. Dudnikov, etc.; Edited by S.A. Belyakov, M.M. Musarsky. M.: Publishing House of Moscow State University, 2002. p. 280.
8. Energy saving in thermal power engineering and thermal technologies: textbook / A. B. Garyaev, I. V. Yakovlev, A.V. Klimenko [et al.]. URL: https://e.lanbook.com/book/362507