



НАУЧНЫЙ  
ФОРУМ  
nauchforum.ru

ISSN: 2542-2162

№22(245)  
часть 2

НАУЧНЫЙ ЖУРНАЛ

# СТУДЕНЧЕСКИЙ ФОРУМ



Г. МОСКВА



*Электронный научный журнал*

# СТУДЕНЧЕСКИЙ ФОРУМ

№ 22 (245)  
Июнь 2023 г.

Часть 2

Издается с февраля 2017 года

Москва  
2023

УДК 08  
ББК 94  
С88

Председатель редколлегии:

**Лебедева Надежда Анатольевна** – доктор философии в области культурологии, профессор философии Международной кадровой академии, член Евразийской Академии Телевидения и Радио.

Редакционная коллегия:

**Арестова Инесса Юрьевна** – канд. биол. наук, доц. кафедры биоэкологии и химии факультета естественнонаучного образования ФГБОУ ВО «Чувашский государственный педагогический университет им. И.Я. Яковлева», Россия, г. Чебоксары;

**Бахарева Ольга Александровна** – канд. юрид. наук, доц. кафедры гражданского процесса ФГБОУ ВО «Саратовская государственная юридическая академия», Россия, г. Саратов;

**Бектанова Айгуль Карибаевна** – канд. полит. наук, доц. кафедры философии Кыргызско-Российского Славянского университета им. Б.Н. Ельцина, Кыргызская Республика, г. Бишкек;

**Волков Владимир Петрович** – канд. мед. наук, рецензент ООО «СибАК»;

**Елисеев Дмитрий Викторович** – канд. техн. наук, доцент, начальник методологического отдела ООО «Лаборатория институционального проектного инжиниринга»;

**Комарова Оксана Викторовна** – канд. экон. наук, доц. доц. кафедры политической экономии ФГБОУ ВО «Уральский государственный экономический университет», Россия, г. Екатеринбург;

**Лебедева Надежда Анатольевна** – д-р филос. наук, проф. Международной кадровой академии, чл. Евразийской Академии Телевидения и Радио;

**Маршалов Олег Викторович** – канд. техн. наук, начальник учебного отдела филиала ФГАОУ ВО «Южно-Уральский государственный университет» (НИУ), Россия, г. Златоуст;

**Орехова Татьяна Федоровна** – д-р пед. наук, проф. ВАК, зав. Кафедрой педагогики ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск;

**Самойленко Ирина Сергеевна** – канд. экон. наук, доц. кафедры рекламы, связей с общественностью и дизайна Российского Экономического Университета им. Г.В. Плеханова, Россия, г. Москва;

**Сафонов Максим Анатольевич** – д-р биол. наук, доц., зав. кафедрой общей биологии, экологии и методики обучения биологии ФГБОУ ВО «Оренбургский государственный педагогический университет», Россия, г. Оренбург;

**С88 Студенческий форум:** научный журнал. – № 22 (245). Часть 2. М., Изд. «МЦНО», 2023. – 72 с. – Электрон. версия. печ. публ. – <https://nauchforum.ru/journal/stud/22>.

Электронный научный журнал «Студенческий форум» отражает результаты научных исследований, проведенных представителями различных школ и направлений современной науки.

Данное издание будет полезно магистрам, студентам, исследователям и всем интересующимся актуальным состоянием и тенденциями развития современной науки.

ISSN 2542-2162

ББК 94  
© «МЦНО», 2023 г.

## Оглавление

<b>Статьи на русском языке</b>	<b>5</b>
<b>Рубрика «Технические науки»</b>	<b>5</b>
ПОВЫШЕНИЕ КАЧЕСТВА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ В СЕТЯХ 0,4 КВ Андреева Алина Андреевна	5
ИССЛЕДОВАНИЕ КОЭФФИЦИЕНТОВ НЕСИММЕТРИИ ПРИ КОМПЕНСАЦИИ РЕАКТИВНОЙ МОЩНОСТИ В ВОЗДУШНЫХ ЛИНИЯХ 0,4 КВ Андреева Алина Андреевна	8
РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО РЕЗУЛЬТАТАМ АУДИТА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ Арзуманян Эрик Араикович	13
ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ Барашенков Михаил Игоревич	16
ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ АУТЕНТИФИКАЦИИ Бойков Илья Александрович Цыганок Дарья Игоревна	19
РАЗРАБОТКА ТИПОВОГО КОМПЛЕКТА ДОКУМЕНТОВ ПО АТТЕСТАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ Быстров Артем Андреевич	22
ОБЩИЕ ТЕХНОЛОГИЧЕСКИЕ СВЕДЕНИЯ О ПРОКАТНОМ СТАНЕ В МЕТАЛЛУРГИЧЕСКОМ ПРОИЗВОДСТВЕ Кайнов Сергей Александрович Ведерников Никита Викторович Лепихин Александр Васильевич	25
АНАЛИЗ ПРОБЛЕМ ИСПОЛЬЗОВАНИЯ ОТЕЧЕСТВЕННЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ В СРЕДЕ ОБУЧЕНИЯ И ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ Ковалев Кирилл Константинович	29
ПРОГРАММА АУДИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПУБЛИЧНЫХ ОБЛАКАХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ИХ ОБРАБОТКИ Кудряшов Дмитрий Петрович	35
ОЦЕНКА РЕЗУЛЬТАТИВНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА Майоров Марсель Сергеевич	40
ТИРАТРОН Павлов Вадим Алексеевич Разумов Данил Владимирович Агунов Эрдем Александрович Павлова Светлана Валерьевна	43
ВЛИЯНИЕ ТЕМПЕРАТУРНОГО РЕЖИМА ПОЖАРА НА ОГНЕСТОЙКОСТЬ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ Рыжова Мария Николаевна Смотрин Константин Александрович	46

ГИДРОЭЛЕКТРОСТАНЦИИ Сидоров Игорь Александрович Лепихин Александр Васильевич	50
ТРАНЗИСТОРНЫЕ УСИЛИТЕЛИ НИЗКОЙ ЧАСТОТЫ Терентьева Татьяна Михайловна Убашиева Татьяна Дабаевна Кондрашева Алеся Ивановна Павлова Светлана Валерьевна	52
МАРКОВСКАЯ МОДЕЛЬ НАДЕЖНОСТИ ДЛЯ СТРОГОЙ АУТЕНТИФИКАЦИИ ПО СЕРТИФИКАТУ ДОСТУПА Цыганок Дарья Игоревна Бойков Илья Александрович	56
РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОГИСТИЧЕСКОЙ КОМПАНИИ СДЭК Шабалин Александр Дмитриевич	59
СОЗДАНИЕ МАКЕТА КОМПЛЕКСА ДЛЯ АВТОМАТИЗАЦИИ ИЗМЕРЕНИЙ ТРАССОВОГО ЗАТУХАНИЯ ПРИ КОНТРОЛЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК Шишмаков Роман Олегович	61
<b>Рубрика «Физико-математические науки»</b>	<b>64</b>
НЕСИММЕТРИЧНЫЙ МУЛЬТИВИБРАТОР-МЕТРОНОМ Виноградов Александр Юрьевич Белобородов Денис Павлович Павлова Светлана Валерьевна	64
СВЕТОДИОДЫ В СВЕТОВОЙ СИГНАЛИЗАЦИИ Хомогоров Артур Максимович Агунов Алексей Александрович Павлова Светлана Валерьевна	67

## СТАТЬИ НА РУССКОМ ЯЗЫКЕ

## РУБРИКА

## «ТЕХНИЧЕСКИЕ НАУКИ»

## ПОВЫШЕНИЕ КАЧЕСТВА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ В СЕТЯХ 0,4 КВ

*Андреева Алина Андреевна*

*магистрант,*

*Орловский государственный университет*

*имени И.С. Тургенева,*

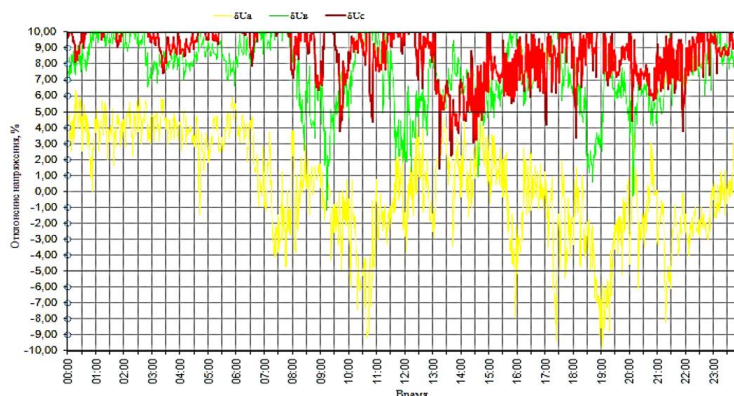
*РФ, г. Орел*

**Аннотация.** В данной статье выполнен анализ влияния несимметрии на потери электрической энергии и работу электрооборудования, а также предложены мероприятия по снижению уровня несимметрии напряжений и токов.

**Ключевые слова:** несимметрия напряжений и токов; коэффициенты несимметрии по нулевой и обратной последовательностям.

В последнее время изменились объемы потребления электрической энергии. Это связано с появлением новых современных электротехнических устройств и систем, оснащенных элементами силовой электроники. Электроприемники потребителя в большинстве своем оказываются высокочувствительными к параметрам качества электрической энергии (ПКЭ) и при этом одновременно могут являться причиной снижения их уровня в электрических сетях. Поставщик электрической энергии (ЭЭ) несет ответственность и гарантирует уровень ПКЭ в соответствии требованиям ГОСТа. Однако качественные показатели ЭЭ в значительной степени снижаются этапах передачи, распределения и потребления энергии.

Для анализа ПКЭ рассмотрим распределительные сети Орловского РЭС. Для проведения контроля ПКЭ производились измерения в течение суток в распределительном устройстве низкого напряжения трансформаторной подстанции ТМ-630/10/0,4. Для измерений был использован регистратор Ресурс-UF2М-3Т52. Результаты измерений регистратора получены в виде таблиц и графиков анализ которых позволил зафиксировать недопустимые отклонения напряжения в двух фазах В и С (см. рисунок 1).



**Рисунок 1. Суточный график отклонений междуфазных напряжений**



Несимметрия характеризуется коэффициентами несимметрии напряжения по нулевой  $K_{0U}$  и обратной  $K_{2U}$  последовательностям. Для электрических сетей общего назначения: значения коэффициентов несимметрии напряжения по обратной и нулевой последовательностям нормально допустимое 2 % и предельно допустимое 4 % [1, 2].

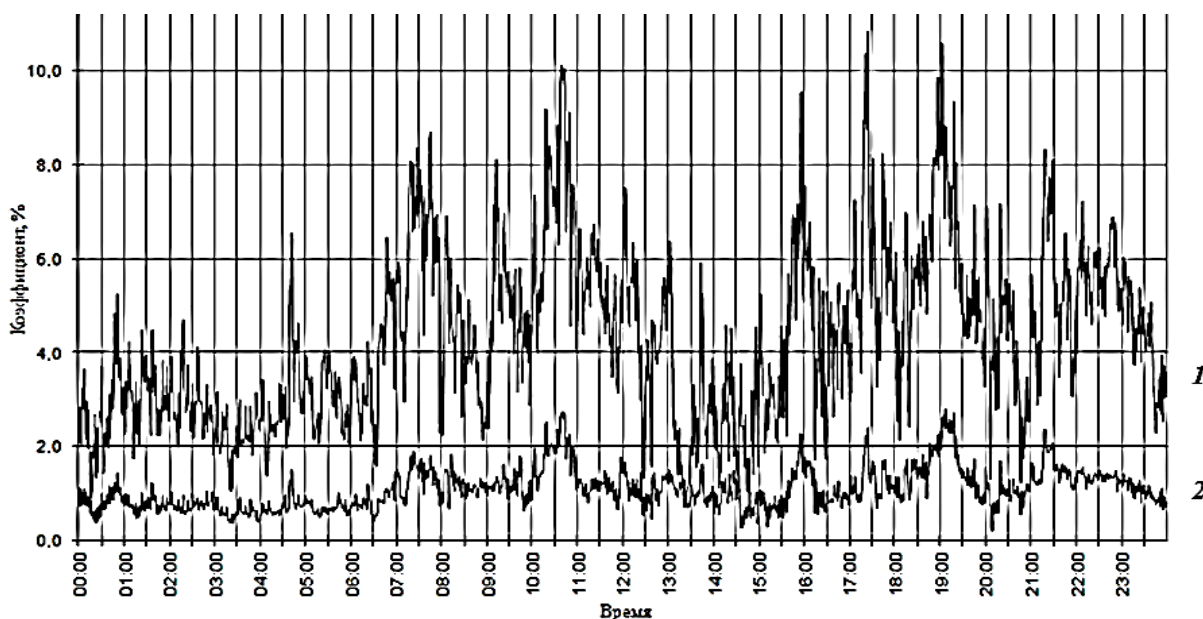
«Коэффициенты несимметрии напряжений по нулевой и обратной последовательности в процентах определяются из выражения:

$$K_{2(0)U} = \frac{U_{0(2)}}{U_{1(1)}} \cdot 100\%,$$

где  $U_{0(2)U}$  – значения напряжений нулевой (обратной) последовательности;

$U_{1(1)}$  – значение напряжения прямой последовательности» [2, 3].

На рисунке 2 приведены графики отклонений коэффициентов несимметрии по нулевой (кривая 1) и обратной (кривая 2) последовательностям.



**Рисунок 2. График суточных значений коэффициентов несимметрии напряжений по нулевой (кривая 1) и обратной (кривая 2) последовательностям**

Из представленных графиков видно, что коэффициент напряжения нулевой последовательности превышает нормируемые ГОСТ 32144–2013 значения, так как в отдельные моменты значительно превышает допустимые 4 %. Максимальное значение  $K_{0U}$  достигало 10,83. Коэффициент напряжения обратной последовательности лишь в течении 4 минут за сутки превысил допустимое значение в 2 %. Максимальное значение  $K_{2U}$  составило 2,41. Можно говорить, что значения коэффициентов несимметрии напряжения по нулевой последовательности превышают более чем в 2,5 раза нормируемые значения.

Результаты выполненного анализа показывают, что обеспечение качества ЭЭ в распределительных сетях низкого напряжения остается достаточно актуальной задачей. Наблюдаются значительные искажения синусоидальности напряжений и в некоторых случаях несимметрия напряжений в несколько раз превышает нормируемые значения. В сетях общего назначения неравномерное распределение однофазных нагрузок потребителей вызывает появление напряжения нулевой последовательности и существенное увеличение тока в нейтральном проводе низковольтной сети. В результате снижается надежность и увеличиваются потери в несимметричных трехфазных сетях и элементах распределения ЭЭ, а также снижается срок службы электрооборудования. В элементах электрических сетей, трансформаторах и электрических двигателях увеличиваются электрические потери и потребляемая мощность [3, 4, 5].

А применение конденсаторных батарей в несимметричной сети может повлечь за собой дополнительное увеличение неравномерности нагрузки фаз.

Наиболее простым решением вопроса симметрирования в сетях 0,4 кВ является перераспределение нагрузок по фазам. Однако, это не всегда представляется возможным. В этом случае для устранения существующего дисбаланса токов и напряжений необходимо использовать балансирующие устройства: специальные филтросимметрирующие и шунтосимметрирующие устройства [6, 7]. Применение устройств симметрирования на базе управляемых силовых MOSFET и IGBT транзисторов обеспечит контроль и управление не только параметрами симметрии токов и напряжений, но и параметрами отклонения напряжения и несинусоидальности [8]. Это позволит привести показатели симметрии напряжений и токов в ТОП в соответствие с нормируемыми значениями, не выполняя дорогостоящих работ, связанных с реконструкцией распределительной сети 0,4 кВ. Также это позволит снизить уровень потерь в распределительных сетях за счет уменьшения токов нулевой и обратной последовательностей.

### Список литературы:

1. ГОСТ 32144-2013. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. – Введ. 2014.07.01. – М. : Стандартиформ, 2013. – 10 с.
2. Дед Александр Евгеньевич. Учет несимметричного характера нагрузки при расчетах потерь мощности в распределительных сетях 0,38 кВ.: дис. Кандидат наук: 05.14.02 – Электростанции и электроэнергетические системы. ФГБОУ ВО «Омский государственный университет». 2018. 247 с.
3. Дулепов Дмитрий Евгеньевич, Тюндина Татьяна Евгеньевна Расчет несимметрии напряжений СЭС // Вестник НГИЭИ. 2015. №4 (47).
4. Шидловский А.Н. Повышение качества энергии в электрических сетях. / А.Н. Шидловский, В.Г. Кузнецов – К.: Наукова думка, 1985. – 268 с.
5. Романова В.В., Хромов С.В., Батухтин А.Г., Суслов К.В. Анализ степени влияния несимметрии питающего напряжения на эксплуатационную надёжность низковольтных асинхронных электродвигателей // Известия высших учебных заведений. ПРОБЛЕМЫ ЭНЕРГЕТИКИ. 2022. Т.24. № 4. С. 131-141.
6. Шидловский, А.К. Оптимизация несимметричных режимов систем электроснабжения. / А.К. Шидловский, В.Г. Кузнецов, В.Г. Николаенко. – Киев.: Наук.думка, 1987. – 176 с.
7. Наумов И.В., Ямщикова И.В. Повышение эффективности режимов работы сетей низкого напряжения России и Германии при несимметричном электропотреблении // Вестник КрасГАУ. 2015. №10.
8. Савина Н.В., Лисогурский И.А., Лисогурская Л.Н. Выбор схемных и технических решений для улучшения качества электроэнергии в адаптивных сетях с тягой переменного тока. Известия высших учебных заведений. ПРОБЛЕМЫ ЭНЕРГЕТИКИ. 2022;24(3):42-54.



## ИССЛЕДОВАНИЕ КОЭФФИЦИЕНТОВ НЕСИММЕТРИИ ПРИ КОМПЕНСАЦИИ РЕАКТИВНОЙ МОЩНОСТИ В ВОЗДУШНЫХ ЛИНИЯХ 0,4 КВ

**Андреева Алина Андреевна**

магистрант,  
Орловский государственный  
университет имени И.С. Тургенева,  
РФ, г. Орел

**Аннотация.** В данной статье приведены результаты исследований коэффициентов несимметрии по нулевой и обратной последовательности при пофазной компенсации реактивной мощности в воздушных линиях 0,4 кВ. По результату исследования видно, что компенсация помогает уменьшить значения коэффициентов несимметрии. Также это приводит к уменьшению потерь.

**Ключевые слова:** Компенсация реактивной мощности, коэффициент несимметрии по нулевой и обратной последовательности.

На сегодняшний день потери электроэнергии в России при ее транспортировке и распределении значительны. Без изменения данной ситуации невозможно говорить про энергоэффективность. Поэтому одной из основных задач является улучшение качества электроэнергии у потребителя. Вся поставляемая электроэнергия, которую получает потребитель, должна удовлетворять требованиям ГОСТ 32144-2013 [2].

Данный стандарт устанавливает показатели и нормы качества электрической энергии в точках ее передачи пользователям электрических сетей низкого напряжения систем электроснабжения общего назначения. К основным показателям качества электроэнергии (КЭ) относят: установившееся отклонение напряжения  $\delta U$ , коэффициенты несимметрии напряжений по обратной  $K_{2U}$ , и нулевой последовательности  $K_{0U}$

Согласно ГОСТу для указанных показателей КЭ установлены нормы «значения коэффициентов несимметрии напряжений по обратной последовательности  $K_{2U}$  и несимметрии напряжений по нулевой последовательности  $K_{0U}$  в точке передачи электрической энергии, усредненные в интервале времени 10 мин, не должны превышать 2 % в течение 95 % времени интервала в одну неделю; – значения коэффициентов несимметрии напряжений по обратной последовательности  $K_{2U}$  и несимметрии напряжений по нулевой последовательности  $K_{0U}$  в точке передачи электрической энергии, усредненные в интервале времени 10 мин, не должны превышать 4 % в течение 100 % времени интервала в одну неделю.»

В данной работе будут рассмотрены результаты исследований коэффициентов несимметрии для нулевой и обратной последовательности с пофазной компенсацией реактивной мощности в сетях 0,4 кВ. Для этого произведем расчет исследуемых коэффициентов до и после компенсации реактивной мощности. Расчет произведем по нижеуказанным формулам.

При компенсации реактивной мощности (КРМ) уменьшается реактивная нагрузка сети, что влечет за собой к изменению напряжения на величину, равную :

$$U_{\text{рег}} = Q_c X_L / U_{\text{ном}}^2 \quad [\text{ОТ. ЕД}] \quad (1)$$

где  $Q_c$  - реактивная мощность компенсирующих устройств (КУ), Вар;

$X_L$  – индуктивное сопротивление участка линии,

Ом – номинальное напряжение сети, В.

Коэффициент несимметрии напряжений по обратной последовательности определяется, % [2]:

$$K_{2U} = U_{2(1)} / U_{1(1)} \cdot 100\% \quad (2)$$

где  $U_{2(1)}$  – действующее значение напряжения обратной последовательности основной частоты трехфазной системы напряжений, В;

$U_{1(1)}$  – действующее значение напряжения прямой последовательности основной частоты, В.

При определении  $U_{2(1)}$  допускается использование приближенной формулы [7]:

$$U_{2(1)} = 0,62 \cdot (U_{нб(1)i} - U_{нм(1)i}) \quad (3)$$

где  $U_{нб(1)i}$ ,  $U_{нм(1)i}$  – наибольшее и наименьшее действующие значения из трех междуфазных напряжений основной частоты в  $i$ -м наблюдении.

Коэффициент несимметрии напряжений по нулевой последовательности определяется, % [2]:

$$K_{0U} = U_{0(1)} / U_{ном.ф} \cdot 100\% \quad (4)$$

где  $U_{0(1)}$  – действующее значение напряжения нулевой последовательности основной частоты трехфазной системы напряжений, В;

$U_{ном.ф}$  – номинальное значение фазного напряжения сети, В.

При определении  $U_{0(1)}$  допускается использование приближенной формулы [7]:

$$U_{0(1)} = 0,62 \cdot (U_{нб.ф(1)i} - U_{нм.ф(1)i}) \quad (5)$$

где  $U_{нб.ф(1)i}$ ,  $U_{нм.ф(1)i}$  – наибольшее и наименьшее действующие значения из трех фазных напряжений основной частоты в  $i$ -м наблюдении.

Потери напряжения в линии можно рассчитать по формуле [3]:

$$\Delta U = S \cdot (r \cos \varphi + x \sin \varphi) / U_{ном} \quad (6)$$

где  $S$  – полная мощность нагрузки;

$r, x$  – сопротивление участка линии;

$\cos \varphi$  – коэффициент мощности нагрузки.

Если таких участков несколько, то потери напряжения на каждом участке суммируются, В:

$$\Delta U = \sum_{i=1}^n \frac{P_i}{\cos \varphi_i \cdot U_{ном}} \cdot (r \cos \varphi_i + x \sin \varphi_i) \quad (6)$$

Где  $P_i / \cos \varphi$  – полная мощность в соответствующей фазе на участке линии, ВА;

$U_i$  – напряжение участка, В;

$r_i, x_i$  – сопротивление участка линии, Ом;

$\cos \varphi_i$  – коэффициент мощности на рассматриваемом участке,  $\sin \varphi_i = \sin(\arccos \varphi_i)$ .

Далее определены значения напряжений в середине линии согласно выражению:

$$U^* = U - \Delta U, \quad (7)$$

Где  $U$  – данные замеров значений фазных напряжений в начале линии.

Таким образом, значения фазных напряжений после КРМ в исследуемой точке линии определены как:

$$U^* = U - \Delta U + U_{per}, \quad (8)$$

Воздушные линии городских и сельских сетей 0,4 кв имеют большую протяженность, что влияет на значения отклонений установившихся значений напряжений в ТОП, а также

превышение нормируемых гостом 32144-2013 значений коэффициентов несимметрии по обратной и нулевой последовательностям.

Как правило, на практике для воздушных линий 0,4 кВ применяются компенсирующие устройства мощностью не превышающей 100 кВАр. Такие устройства имеют небольшой вес и габариты, что позволяет их располагать в соответствующем корпусе на опорах линий электропередач.

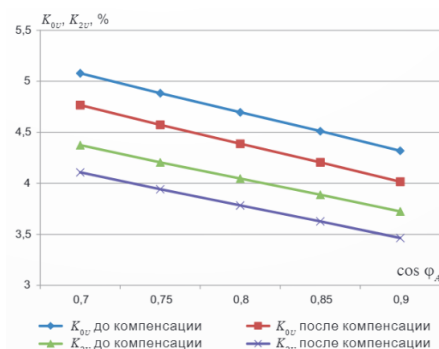
В работе исследована степень влияния пофазной компенсации реактивной мощности на коэффициенты несимметрии напряжений. В таблице 1 приведены результаты расчетов напряжений и коэффициентов несимметрии до и после компенсации в зависимости от коэффициента мощности в одной из фаз при неизменном значении коэффициента мощности.

Активная мощность для двух фаз взята равной 2,255 кВт, для фазы А – 4 кВт, длина участка линии равна 1 км. При расчете потерь напряжения, согласно выражению (6), сопротивления участков линии взяты с учетом сопротивления провода А-50, который наиболее часто встречается в сетях 0,4 кВ. Напряжения в начале линии взяты равными  $U_A = 233,39$  В;  $U_B = 241,20$  В;  $U_C = 242,10$  В.

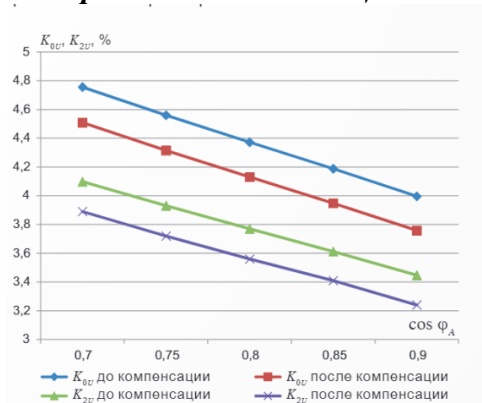
На рисунке 1 приведены графики зависимости коэффициентов несимметрии напряжения по нулевой и обратной последовательности от коэффициента мощности для значений из таблицы 1.

В таблице 2 приведены результаты расчета со значением коэффициента мощности в двух фазах до компенсации, равным 0,8, при различных значениях коэффициента мощности в третьей фазе.

На рисунке 2 приведены графики зависимости коэффициентов несимметрии напряжения по нулевой и обратной последовательности от коэффициента мощности для значений из таблицы 2.



**Рисунок 1. Графики зависимости коэффициентов несимметрии напряжения по нулевой и обратной последовательности от коэффициента мощности по результатам расчетов из таблицы 1**



**Рисунок 2. Графики зависимости коэффициентов несимметрии напряжения по нулевой и обратной последовательности от коэффициента мощности по результатам расчетов из таблицы 2**

Таблица 1.

## Результат расчета по КМР по одной фазе

Cosφ	До компенсации				После компенсации			
	U <sub>0(1)</sub> , В	K <sub>0(U)</sub> , %	U <sub>2(1)</sub> , В	K <sub>2(U)</sub> , %	U <sub>0(1)</sub> , В	K <sub>0(U)</sub> , %	U <sub>2(1)</sub> , В	K <sub>2(U)</sub> ,
0,7	11,65	5,05	10,05	4,37	10,95	4,68	9,44	4,10
0,75	11,22	4,98	9,66	4,20	10,50	4,55	9,05	3,93
0,8	10,85	4,74	9,30	4,01	10,25	4,29	8,65	3,75
0,85	10,27	4,52	8,97	3,75	9,98	4,20	8,25	3,62
0,9	9,08	4,22	8,55	3,69	9,85	3,98	7,95	1,42

Таблица 2.

## Результат расчета по КМР во всех фазах

Cosφ	До компенсации				После компенсации			
	U <sub>0(1)</sub> , В	K <sub>0(U)</sub> , %	U <sub>2(1)</sub> , В	K <sub>2(U)</sub> ,	U <sub>0(1)</sub> , В	K <sub>0(U)</sub> , %	U <sub>2(1)</sub> , В	K <sub>2(U)</sub> ,
0,7	10,95	4,75	9,42	4,09	10,33	4,49	8,92	3,85
0,75	10,39	4,55	9,02	3,95	9,92	4,25	8,55	3,70
0,8	10,05	4,27	8,65	3,66	9,65	4,10	8,20	3,54
0,85	9,62	4,18	8,30	3,59	9,25	3,96	7,85	3,39
0,9	9,18	4,05	7,95	3,48	8,73	3,85	7,30	3,27

Проанализировав результаты, можно отметить снижение коэффициентов несимметрии напряжений по обратной и нулевой последовательности после компенсации реактивной мощности. Это приводит к снижению потерь электроэнергии, а также снижению общих потерь электроэнергии при компенсации реактивной мощности.

### Заключение

Из анализа результатов расчетов, приведенных в таблицах и графиках, следует, что после компенсации значения несимметрии напряжений по обратной и нулевой последовательности уменьшаются.

Степень уменьшения коэффициентов несимметрии по обратной и нулевой последовательности будет зависеть в основном от реактивной мощности компенсации. Поскольку эта величина зависит от коэффициента мощности и передаваемой активной мощности в данной точке линии, то и возможная степень уменьшения исследуемых коэффициентов будет зависеть от вышеперечисленных параметров.

В работе были проведены аналогичные расчеты с другими значениями исходных фазных напряжений, имеющих меньшую несимметрию. При этом были получены аналогичные в приведенных таблицах результаты, подтверждающие наблюдаемый эффект.

Следовательно, при пофазной КРМ положительный эффект уменьшения коэффициентов несимметрии напряжений будет иметь место при любых значениях несимметрии напряжений. Уменьшение коэффициента несимметрии напряжений по нулевой последовательности, как известно, влечет уменьшение токов нулевой последовательности, протекающих в нулевом проводе. Это приводит к уменьшению потерь электроэнергии и может учитываться как дополнительный положительный вклад в уменьшение общих потерь электроэнергии при КРМ.

### Список литературы:

1. Энергетическая стратегия России на период до 2030 года. Министерство энергетики РФ.  
URL: <https://minenergo.gov.ru/node/1026>

2. ГОСТ 32144-2013. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. URL: <http://docs.cnid.ru/document/1200104301>
3. Карташев И.И., Тульский В.Н. и др.; под ред. Шарова Ю.В. Управление качеством электроэнергии. М.: Издательский дом МЭИ, 2008. 354 с
4. Карчин В.В. Локальная компенсация реактивной мощности в сельских распределительных сетях 0,4 кВ. Электрооборудование: эксплуатация и ремонт, 2014, №2 11С. 21-24.
5. Карчин В.В. Сидорова В.Т., Федотов А.И. Компенсация реактивной мощности в сельских распределительных сетях 0,4 кВ для улучшения качества электроэнергии. Известия высших учебных заведений. Проблемы энергетики 2015, №5-6 С. 101-106.

## РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО РЕЗУЛЬТАТАМ АУДИТА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

*Арзуманян Эрик Араикович*

*магистрант,*

*Московский институт электронной техники,*

*РФ, г. Москва*

Методические рекомендации давались по результатам аудита инфраструктуры открытых ключей компании АО «НК «НЕФТЕГАЗ»

На данный момент в АО «НК «НЕФТЕГАЗ» отсутствует собственный УЦ, а также нет производственной необходимости в его внедрении. АО НК «НЕФТЕГАЗ» сотрудничает с УЦ Такском в части выпуска усиленных квалифицированных ЭП. В течение года в среднем выпускаются 30 сертификатов. В перспективе это число может вырасти. При учете дочерних и связанных обществ АО «НК «НЕФТЕГАЗ» количество может возрасти до 300 сертификатов.

Во всех ситуациях, специально не предусмотренных Федеральными законами или иными нормативными правовыми актами, работники АО НК «НЕФТЕГАЗ» применяют простую ЭП.

ЭП в АО «НК «НЕФТЕГАЗ» используется для решения следующих задач:

- Обеспечение юридически значимого электронного документооборота в информационной системе 1С;
- Возможность участия в тендерах, аукционах, закупках и котировках на электронных площадках;
- Создание VPN-соединений для установления удаленного доступа.

В настоящее время в АО «НК «НЕФТЕГАЗ» работа с ЭП регламентируется в документе «Положение об ЭП». «Положение об ЭП», утвержденное приказом АО «НК «НЕФТЕГАЗ» от 14 октября 2021 г. №34, является локальным нормативным актом постоянного действия. Область действия данного документа распространяется на всех сотрудников компании, использующих ЭП при выполнении своих должностных обязанностей. В нем перечислены общие положения, порядок использования и выдачи ЭП и меры обеспечения безопасности. По предоставленной информации часть требований и рекомендаций данного положения не исполняется.

Другие документы или инструкции, описывающие взаимодействие сотрудников с ЭП в компании, отсутствуют [1].

Сведения о нормативно-методических документах, на основании которых разработан перечень документов, необходимых для организации работы с сертификатами и ключами КЭП, приведен в таблице (см. Таблица ) [2]:

*Таблица 1.*

### Нормативно-методические документы, на основании которых разработан перечень документов, необходимых для организации работы с сертификатами и ключами КЭП

№ п/п	Наименование документа
1.	Федеральный закон (ФЗ) от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».
2.	«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства Российской Федерации от 01.11.2012 № 1119.
3.	«Требования к средствам электронной подписи» и «Требования к средствам удостоверяющего центра», утвержденные приказом ФСБ России от 27 декабря 2011 г. № 796.
4.	Руководящий документ ФСБ России от 31.01.2014 № 149/7/1/3-58 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования».

№ п/п	Наименование документа
5.	Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (далее – Приказ ФСБ от 09.02.2005 N 66)
6.	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
7.	ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
8.	ГОСТ 2.106-96. «Межгосударственный стандарт. Единая система конструкторской документации. Текстовые документы».
9.	ГОСТ 2.105-2019. «Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам».
10.	ГОСТ 34.201-89. «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
11.	ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».
12.	ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы-стадии создания».
13.	ГОСТ 34.603-92. «Информационная технология. Виды испытаний автоматизированных систем».
14.	ГОСТ 34.003-90. «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
15.	РД 50-682-89. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».

Согласно пункту 26 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты [3].

На основании этого в компании рекомендуется разработать и внедрить следующие документы:

- Приказ о назначении администратора информационной безопасности;
- Инструкция администратора информационной безопасности.

Также согласно пункту 7 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» орган криптографической защиты осуществляет:

- Проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломб), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ). Готовность обладателей конфиденциальной информации к самостоятельному использованию подтверждается подписанным актом о вводе в эксплуатацию СКЗИ.



- Разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

- Обучение лиц, использующих СКЗИ, правилам работы с ними. Обучение лиц, использующих СКЗИ подтверждается подписанным актом об ознакомлении с Инструкцией пользователя ЭП.

- Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним.

- Учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ.

Согласно пункту 26 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

Согласно пункту 48 Приказа ФСБ от 09.02.2005 N 66 СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

На основании этих пунктов в АО НК «НЕФГАЗ» рекомендуется разработать и внедрить следующие документы:

- Приказ о порядке хранения и эксплуатации средств криптографической защиты информации;

- Приказ о назначения пользователя ЭП;

- Форма перечня сотрудников, допущенных к работе с СКЗИ;

- Форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- Инструкция по реагированию на инциденты информационной безопасности;

- Инструкция пользователя ЭП.

Согласно пункту 46 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом.

На основании этого в компании рекомендуется разработать и внедрить следующий документ:

- Форма акта об уничтожении криптографических ключей и ключевых документов.

### Список литературы:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-99. □ Введ. 2000-01-01. – М.: Изд-во стандартов, 1999. – 11 с.
3. Об информации, информационных технологиях и о защите информации: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г.]. – URL: <http://www.rg.ru/gazeta/rg/2006/07/29> (дата обращения: 18.04.2017).

## ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ

**Барашенков Михаил Игоревич**

*магистрант,*

*Московский институт электронной техники,*

*РФ, г. Москва*

В сфере информационной безопасности основными задачами является сохранять свойства информации, обеспечивать целостность данных, их конфиденциальность и доступность. Это достигается использованием средств защиты информации или принятием управленческих решений, например, проведением мероприятий по повышению информационной безопасности путем повышения осведомленности сотрудниками компании. Важными задачами для компании с точки зрения определения зрелости в сфере безопасности информации является проведение анализа рисков информационной безопасности и оценка эффективности защиты информации. Риск зависит от реализации причинения ущерба, а также зависит от его размера, в случае осуществления угрозы.

Путем анализа риска информационной безопасности выделяются активы, которые необходимо защитить, и определяются угрозы для данных активов. Могут быть выявлены критические процессы или факторы, которые несут негативный характер для бизнес-процессов компании.

Для обеспечения информационной безопасности в организации определяются границы, которые указывают на опасность той или иной угрозы. После этого шага необходимо проанализировать риски и идентифицировать угрозы, т.е. насколько большой ущерб может нанести угроза. На этом же этапе выявляются возможные уязвимости и слабые места в системе, проводится подсчет риска. Это реализуется с помощью методов качественной и количественной оценки. Данные методы указывают на показатели ресурсов и эффективность уже имеющихся средств защиты информации или информационных систем в целом [1].

Для всех мероприятий, связанных с рисками, главная задача представляет собой обеспечение целостности и доступности информации. Нарушение свойств информации может происходить по разным причинам, например:

следствие преднамеренных действий;

физические воздействия;

сбой оборудования;

ошибки в ПО [2].

Главной задачей информационной безопасности организации является управление рисками нарушения информационной целостности, а ее обеспечение – это главный критерий качества выполнения информационных процессов, в том числе и информационной инфраструктурой организации в целом [3].

Анализ рисков информационной безопасности дает возможность определить достаточные и необходимые средства для уменьшения рисков и увеличения защищенности информации компании. Оценка эффективности защиты информации позволяет скорректировать уровень риска безопасности, а также оценить необходимые действия, направленные на повышение защищенности информации. Это позволит увидеть пути минимизирования уязвимостей и общего ущерба рисков информационной безопасности, что в свою очередь усилит показатели защищенности информации в компании.

Проведение оценки эффективности является важным и системным процессом получения объективной оценки состояния системы. Проводится мониторинг заранее установленных действий, направленных на уменьшение рисков информационной безопасности. Оценку эффективности защиты информации необходимо проводить на этапе разработки системы защиты информации и в процессе эксплуатации, для получения оптимальных показателей работы системы в целом [4].

При помощи одного показателя невозможно достаточно точно дать характеристику методике, в которой определяется эффективность комплексной системы защиты информации организации. При оценке эффективности защиты, в зависимости от применяемых способов и показателей получения, выделяют несколько подходов.

Классический подход к оценке эффективности подразумевает использование критериев эффективности, получаемых из показателей эффективности, при создании или модификации системы защиты информации. Показатели эффективности получают путём анализа свойств и характеристик действующей автоматизированной системы. Из-за наличия большого количества неопределённых данных, сложности описания и формализации процессов, отсутствия общих методов вычисления показателей эффективности возникают трудности по использованию классического подхода в качестве методов оценки эффективности защиты информации.

Экспериментальный подход – оценка эффективности происходит путем преодоления элементов системы защиты разработчиками этой системы, которые выступают в роли злоумышленников. То есть имитируются действия злоумышленника с различными навыками, умениями и возможностями, начиная от неопытного злоумышленника и заканчивая высококвалифицированным профессионалом.

Для оценки эффективности защиты необходимо выбрать идеальные значения этой оценки для сравнения и определения удовлетворения сравниваемым системам относительно системы, принимаемой за нормативную. В дополнение к этому подходу можно использовать несколько подходов, которые могут быть применены в определенном случае при их дифференцированном применении. Таким случаем приводится к сравнению с показателями, определяющими эффективность эталонного образца защиты системы. Этот эталонный образец может быть создан с использованием всех современных методов и средств проектирования систем защиты информации, включая методы и средства других организаций.

Однако могут возникнуть трудности использования указанных подходов. В таком случае используется метод экспертных оценок. Данный представляет собой процедура получения оценки проблемы на основе мнения специалистов (экспертов) с целью последующего принятия решения (выбора). Так же экспертная оценка является составным элементом комплексной оценки эффективности механизма защиты системы, использующая все подходы к отдельным субъектам подсистемы, так и всей системы в целом [6].

Для проведения оценки эффективности необходимо создать правило предпочтения, основанное на показателях эффективности – критерий эффективности. Для получения критерия эффективности при использовании некоторого множества показателей используют ряд подходов.

1. Определяется наиболее важный показатель, в таком случае оптимальной будет считаться такая система защиты, где этот показатель достигает наивысшего значения, при том, что остальные показатели удовлетворяют оставшимся условиям, заданным в виде определенных неравенств для оставшихся показателей.

2. Ранжирование всех показателей по важности и при сравнении систем одинаковые показатели сравниваются по убыванию их важности.

Для определения оценки эффективности защиты информации необходимо использование различных множеств характеристик, что невозможно оценить при помощи одного показателя эффективности. Поэтому использование при оценке эффективности множество показателей будет характеризовать эффективность более подробно.

### **Список литературы:**

1. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации // Вопросы защиты информации. – 2014. – № 1(104).
2. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Сер. 3: Образовательные ресурсы и технологии. 2015. № 1(9). С. 73-79.

3. Нарушение целостности, работоспособности системы. URL: [https://studopedia.ru/14\\_114815\\_narushenie-konfidentsialnosti-tselostnosti-rabotosposobnosti-sistemi.html](https://studopedia.ru/14_114815_narushenie-konfidentsialnosti-tselostnosti-rabotosposobnosti-sistemi.html)
4. Анализ и оценка рисков в бизнесе : учебник и практикум для СПО / Т.Г. Касьяненко, Г.А. Маховикова. 2-е изд., пер. и доп. М. : Юрайт, 2019. 381 с.
5. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: [https://elar.urfu.ru/bitstream/10995/50431/1/m\\_t\\_h\\_k.a.krinitsyn\\_2017.pdf](https://elar.urfu.ru/bitstream/10995/50431/1/m_t_h_k.a.krinitsyn_2017.pdf)
6. Баранова Е.К., Бабаш Л.В. Информационная безопасность и защита информации: Учеб. пособие. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2016. 322 с.
7. Управление рисками при внедрении информационных технологий на промышленных предприятиях. URL: <https://goo.su/ItN>
8. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: <https://web.snauka.ru/issues/2020/01/90380>

## ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ АУТЕНТИФИКАЦИИ

**Бойков Илья Александрович**

студент,  
Московский государственный технический  
университет им. Н.Э. Баумана,  
РФ, г. Москва

**Цыганок Дарья Игоревна**

студент,  
Московский государственный технический  
университет им. Н.Э. Баумана,  
РФ, г. Москва

В современном цифровом мире аутентификация играет решающую роль в защите данных и контроле доступа к ресурсам. Традиционные системы аутентификации, хоть и эффективны, но в некоторых случаях, все же имеют свои ограничения и уязвимости. Однако с появлением блокчейн-технологий открываются новые перспективы для повышения надежности и безопасности процесса аутентификации. Блокчейн, с его уникальными особенностями и преимуществами, предоставляет инновационный подход к решению проблем, связанных с аутентификацией и контролем доступа.

Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации [1].

Блокчейн – это децентрализованная база данных, в которой все записи собираются в блоки и связываются между собой средствами криптографии. [2]

Основными преимуществами использования блокчейн-технологий для аутентификации является:

Отсутствие единой точки контроля: Блокчейн предполагает разбитую на узлы структуру, что означает отсутствие единого контролирующего органа. Это предотвращает манипуляцию данными и устраняет единую точку отказа, что увеличивает безопасность системы аутентификации и контроля доступа.

Неподдельность и прозрачность: Блокчейн обеспечивает неподдельность и прозрачность действий, так как копии всех записей хранятся в нескольких местах сети. Это гарантирует, что данные об аутентификации и доступе не могут быть изменены или удалены без обнаружения.

Устойчивость к атакам: благодаря криптографическому хэшированию и механизму согласования между узлами сети, блокчейн сложно атаковать или взломать. Даже если злоумышленник сможет атаковать один узел, другие узлы в сети продолжают функционировать, обеспечивая стабильность системы.

Автоматизация процессов: Смарт-контракты – компьютерная программа, которая выполняет соглашения, заключенные между двумя и более сторонами, в результате которых, при выполнении тех или иных условий происходят определенные действия. [3] Они позволяют автоматизировать процессы аутентификации и управления доступом. Это упрощает процедуры и сокращает время, необходимое для предоставления доступа к данным.

Сравним системы аутентификации с использованием блокчейн-технологии и без неё.

Таблица 1.

**Сравнение систем аутентификации**

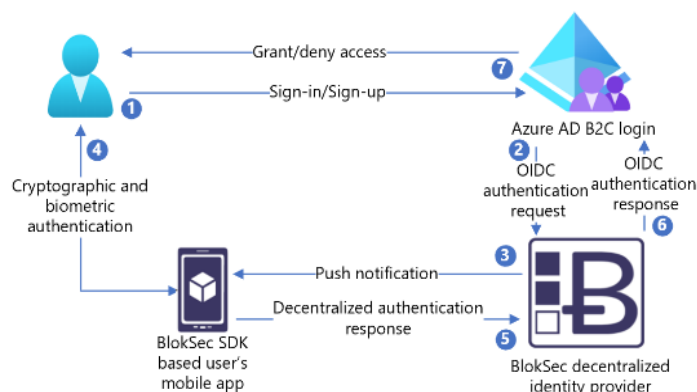
<b>Критерий сравнения</b>	<b>Блокчейн-технология</b>	<b>Традиционная система аутентификации</b>
Безопасность	Высокая, благодаря криптографическим методам и отсутствию единого контролирующего центра	Зависит от реализации и архитектуры системы, но может быть более уязвима для атак
Приватность	Высокая, пользователи контролируют свои данные и разрешения	Зависит от политики конфиденциальности поставщика услуг, но данные обычно централизованы и могут быть уязвимы для утечек
Скорость и производительность	Может быть ниже из-за согласования между узлами	Обычно выше, так как основана на централизованных серверах
Удобство использования	Менее удобна для непрофессиональных пользователей, требует адаптации	Широко распространена, привычна и удобна для большинства пользователей
Масштабируемость	Зависит от алгоритма согласования и архитектуры блокчейн-сети	Обычно масштабируется легче, так как основана на централизованных серверах
Стоимость и экономическая эффективность	Может быть выше из-за расходов на достижение согласия между узлами и поддержание сети без централизованного контроля	Обычно ниже, так как основана на централизованных серверах и не требует дополнительных расходов на консенсус

Однако стоит отметить, что конкретные характеристики каждой системы могут варьироваться в зависимости от реализации и архитектуры и каждый случай стоит рассматривать индивидуально.

Преимущество использования блокчейн-технологии для аутентификации заключается в том, что пользователь передает не свои данные, а только хэш. Утечка информации с блока не критична, так как хэш-функции являются односторонними, что означает, что восстановить исходные данные из хэша практически невозможно. Это обеспечивает дополнительный уровень защиты конфиденциальности данных пользователя в публичном облаке.

Подробнее про работу данной технологии можно узнать из документации Microsoft, которая одна из первых предложили использовать данное решение, описали принцип ее интеграции в свои проекты и показали ее работу. [4]

Рассмотрим процесс регистрации и входа:



**Рисунок 1. Поток регистрации и входа в реализацию решения BlokSec**

1. Пользователь входит в приложение Azure AD B2C и пересылается в Azure AD политике входа и регистрации B2C.

2. Azure AD B2C перенаправляет пользователя на маршрутизатор удостоверений BlokSec с помощью потока кода авторизации OIDC, который не зависит от единого контролирующего центра.

3. Маршрутизатор BlokSec отправляет push-уведомление в мобильное приложение пользователя с сведениями о проверке подлинности и запросе на авторизацию.

4. Пользователь проверяет запрос проверки подлинности. Принятому пользователю предлагается выполнить биометрию, например отпечаток пальца или сканирование лица.

5. Ответ имеет цифровую подпись с помощью уникального цифрового ключа пользователя. Ответ проверки подлинности предоставляет подтверждение владения, присутствия и согласия. Ответ возвращается маршрутизатору.

6. Маршрутизатор проверяет цифровую подпись на соответствие неизменяемому уникальному открытому ключу пользователя, хранящемуся в базе, которая синхронизирована между всеми участниками сети. Маршрутизатор отвечает на Azure AD B2C с результатом проверки подлинности.

7. Пользователю предоставляется или запрещается доступ.

Использование Azure AD B2C с BlokSec для аутентификации без пароля предлагает ряд значительных преимуществ, которые улучшают безопасность и удобство использования. Основное преимущество этой системы – повышение уровня безопасности. Отсутствие необходимости в паролях значительно уменьшает вероятность их угадывания или воровства.

Благодаря данному подходу пользователи могут легко войти в систему без необходимости помнить сложные пароли. Вместо этого они используют такие биометрические данные, как отпечаток пальца или сканирование лица, что обеспечивает удобство использования.

Таким образом, блокчейн-технологии представляют собой инновационный и многообещающий подход к обеспечению надежности и безопасности в процессе аутентификации. Они преодолевают ограничения традиционных систем аутентификации и предлагают новые возможности для защиты данных и контроля доступа в современном цифровом мире.

### Список литературы:

1. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация // Электронный фонд правовых и нормативно-технических документов URL: <https://docs.cntd.ru/document/1200172576> (дата обращения: 20.05.2023)
2. Технология блокчейн с точки зрения информационной безопасности. Часть 1 // Меню Интернет-портал по информационной безопасности в сети URL: <https://safe-surf.ru/specialists/article/5278/658923/> (дата обращения: 25.05.23).
3. Автономность и безопасность. Как работают смарт-контракты // РБК URL: <https://clck.ru/34fhiR> (дата обращения: 25.05.23).
4. Руководство: настройка Azure Active Directory B2C с BlokSec для проверки подлинности без пароля // Learn.Microsoft.com URL: <https://learn.microsoft.com/ru-ru/azure/active-directory-b2c/partner-bloksec?pivots=b2c-user-flow> (дата обращения: 23.05.2023).



## РАЗРАБОТКА ТИПОВОГО КОМПЛЕКТА ДОКУМЕНТОВ ПО АТТЕСТАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

**Быстров Артем Андреевич**

магистрант,

Московский институт электронной техники,

РФ, г. Москва

Комплект документов по аттестации государственной информационной системы основывается на ГОСТ РО 0043-004-2013 Программа и методики аттестационных испытаний и составляется на основании испытаний, приведенных в данном регламентирующем документе [1].

Он определяет основные организационно-методические вопросы проведения и обеспечения аттестационных испытаний на соответствие требованиям по безопасности информации объекта информатизации Заказчика – государственной информационной системы.

В первую очередь, в документе указывается сам объект исследования: какая будет государственная информационная система, ее наименование, какие компоненты у нее и где они находятся. Также указывается перечень объектов аттестационных испытаний, где указывается сам объект, класс информации, вид информации, класс защищенности ИС, требуемый уровень защищенности.

Пример на основе Заказчика «Московская библиотека»:

Объектом аттестационных испытаний является ГИС МБ – распределенная информационная система. Перечень объектов аттестационных испытаний указан в таблице 3. В столбце «Класс защищенности ИС» указан класс на основании Приказа ФСТЭК №17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В столбце «Требуемый уровень ПДн» указан уровень защищенности на основании постановления правительства Российской Федерации №1119 от 01.11.2012 г. Перечень объектов аттестационных испытаний приведен в таблице 1.

*Таблица 1.*

**Перечень объектов аттестационных испытаний**

№ п/п	Объект аттестационных испытаний	Класс информации	Вид информации	Класс защищенности ИС	Требуемый уровень защищённости ПДн
1.	ГИС МБ	Персональные данные	обрабатываемая	класс К2	3-й уровень защищённости

Состав ОИ СС ГИС МБ:

- 9 физических серверов;
- виртуальные серверы приложений (17 шт.), виртуальные инфраструктурные серверы (2 шт.), виртуальные и физические серверы СЗИ (3 шт.);
- коммутационное оборудование.

После указания всей информации об объекте аттестационных испытаний прописывается сама цель испытаний. В большинстве случаев указывается на соответствие требованиям какого документа проводилась аттестация, в рамках данной ВКР подготавливались документы по аттестации Московской библиотеки на соответствие приказу ФСТЭК №17. Также указываются задачи проведения испытаний. В общих положениях указывается информация на основании с каким Государственным контрактом и договором проводились испытания. Указывается комиссия аттестации и указание на то, что компания имеет лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации [2].

Для проведения аттестационных испытаний комиссии АО «Аттестация» представляется комплект исходных данных и документация по объектам информатизации, включая:

- технический паспорт на ОИ;
- акты определения уровня защищённости персональных данных ОИ;
- приказ о назначении ответственного за организацию обработки персональных данных на ОИ;
- положение по организации и проведению работ по обеспечению безопасности информации конфиденциального характера (в том числе ПДн) при её обработке в ГИС МБ;
- инструкция по организации охраны и допуску в режимные помещения, в которых эксплуатируются СКЗИ, предназначенные для защиты информации, передаваемой по каналам связи в рамках администрирования ГИС МБ;
- приказ о назначении администратора безопасности ОИ;
- копии или оригиналы лицензионных соглашений, наклейки и т.п. на программные средства, используемые на ОИ;
- копии или оригиналы сертификатов соответствия ФСБ России и ФСТЭК России на применяемые средства защиты информации, используемые в ГИС МБ;
- перечень защищаемой информации, циркулирующей (хранящейся, обрабатываемой) на ОИ;
- приказ о допуске сотрудников к обработке защищаемой информации;
- проектная и эксплуатационная документация на СЗИ ГИС МБ;
- описание технологического процесса обработки информации на ОИ;
- план контролируемой зоны объекта;
- схемы размещения технических средств ОИ;
- организационно-распорядительную документацию разрешительной системы доступа персонала на ОИ;
- инструкции по эксплуатации СЗИ ГИС МБ.

Объем аттестационных испытаний определяется методикой, согласно которой выполняются проверки на соответствие требованиям технического задания (ТЗ) и нормативной документации функций, реализуемых отдельными компонентами, входящими в состав СЗИ ГИС МБ. В рамках составления данного документа для заказчика «Московская библиотека» будет приведена таблица с программой аттестации. Фрагмент приведен ниже, проверка состава СЗИ, входящих в состав СЗИ ГИС МБ. Программа и методика испытаний тесно связаны друг с другом. Сразу же после программы идет методика испытаний, где указано наименование проверки, методика проверки и сам результат [3].

Объем аттестационных испытаний определяется методикой, согласно которой выполняются проверки на соответствие требованиям технического задания (ТЗ) и нормативной документации функций, реализуемых отдельными компонентами, входящими в состав СЗИ ГИС МБ. В общих положениях указывается информация на основании с каким Государственным контрактом и договором проводились испытания. Фрагмент методики проведения испытаний ГИС МБ представлен в таблице 2.

Таблица 2.

## Методики проведения испытаний

№	Наименование проверки	Методика проверки	Результат проверки
Проверка состава СЗИ, входящих в ГИС МБ			
п. 6.3	ОС «РЕД ОС»	Проверка соответствия ОС «РЕД ОС», установленной на серверы, заключается в сравнении установленной версии с версией ОС «РЕД ОС», указанной в эксплуатационной документации на ГИС МБ. Итоговая контрольная сумма дистрибутивных файлов снимается в ОС Windows.	Проверка считается выполненной успешно, если в ходе проверки выявлено соответствие установленной версии ОС «РЕД ОС», версии, указанной в эксплуатационной документации на ГИС МБ.
п. 6.4	ПК «Битрикс»	Проверка соответствия версии ПК «Битрикс», заключается в сравнении установленной версии с версией ПК «Битрикс» указанной в эксплуатационной документации на ГИС МБ.	Проверка считается выполненной успешно, если в ходе проверки выявлено соответствие установленной версии ПК «Битрикс», версии, указанной в эксплуатационной документации на ГИС МБ.

## Список литературы:

1. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. – М.: Форум, Инфра-М, 2020. – 368 с.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2018. – 336 с.
3. Шунейко, А.А. Информационная безопасность человека. Учебное пособие для вузов / А.А. Шунейко. – М.: Владос, 2018. – 119 с.

## ОБЩИЕ ТЕХНОЛОГИЧЕСКИЕ СВЕДЕНИЯ О ПРОКАТНОМ СТАНЕ В МЕТАЛЛУРГИЧЕСКОМ ПРОИЗВОДСТВЕ

**Кайнов Сергей Александрович**

студент

Лысьвенского филиала ФГАОУ ВО Пермского национального  
исследовательского политехнического университета,  
РФ, г. Лысьва

**Ведерников Никита Викторович**

студент

Лысьвенского филиала ФГАОУ ВО Пермского национального  
исследовательского политехнического университета,  
РФ, г. Лысьва

**Лепихин Александр Васильевич**

научный руководитель,

старший преподаватель Лысьвенского филиала ФГАОУ ВО Пермского  
национального исследовательского политехнического университета,  
РФ, г. Лысьва

**Аннотация.** В данной статье рассмотрены основные работы металлургической промышленности прокатного производства рессор, а также рассмотрения процессов и оборудования при термической обработке рессорных листов, создание комплексных линий по отдельным операциям и в целом по технологическому процессу изготовления.

**Ключевые слова:** технологический процесс, прокатный стан, термическая обработка

Авторессорное производство на Пермском заводе является самым современным в России, оснащено высокопроизводительным оборудованием, позволяющим выпускать широкий ассортимент высококачественной рессорной продукции. В цехе разрабатываются новые технологии производства, новые виды рессор.

Программа развития рессорного производства предполагает создание и освоение энергосберегающих и ресурсосберегающих технологий и оборудования. Наиболее перспективное решение – переход на малолитровые (параболические) рессоры, состоящие из одного-четырёх листов продольно-переменного профиля, что позволяет снизить металлоёмкость и трудоемкость изготовления рессор, делает экономичным применение различных методов обработки поверхности рессорных листов, а отсутствие межлистового трения по большей части длины листов существенно увеличивает срок службы рессор. Разработка и освоение именно таких рессор, а также внедрение новых процессов и оборудования при термической обработке рессорных листов, создание комплексных линий по отдельным операциям и в целом по технологическому процессу изготовления рессор являются в условиях развития автомобильной промышленности важнейшей необходимостью.[1]

В металлургической промышленности прокатное производство является одним из основных технологических процессов обработки металла давлением. Физическим процессом, лежащим в процессе прокатного производства, является пластическая деформация металла между вращающимися валками прокатного стана. Процесс прокатки различается по температурному состоянию прокатываемого металла. Горячая прокатка происходит при подаче в валки стана предварительно нагретого металла. К станам горячей прокатки относятся заготовочные, крупносортовые, средние – и мелкосортные, толстолистовые и др. В состав прокатного цеха входят прокатный стан, механизмы для подготовки металла к прокатке, обработка готовой продукции, различные вспомогательные службы. Прокатный стан – сложное устройство,

состоящее из многих механизмов, объединенных одной технологической линией. В прокатном стане имеются главные механизмы – рабочие валки прокатной клетки, которые обеспечивают обжатие металла и придают ему требуемое сечение и форму готовой продукции. К оборудованию главных механизмов относятся приводные двигатели валков и передаточные устройства – редукторы и шестеренные клетки. Вспомогательные механизмы предназначены для перемещения рабочих валков, транспортировки и резки металла и других операций, обеспечивающих определенную последовательность технологического процесса.

Электродвигатели и преобразовательные агрегаты прокатных станов со всем относящимся к ним оборудованием устанавливают в специальных помещениях, которые называются машинными залами. В помещении машинного зала располагается также распределительное устройство высокого напряжения и щит управления прокатными двигателями. Машинный зал располагается в пролете, соседнем с пролетом прокатного стана.

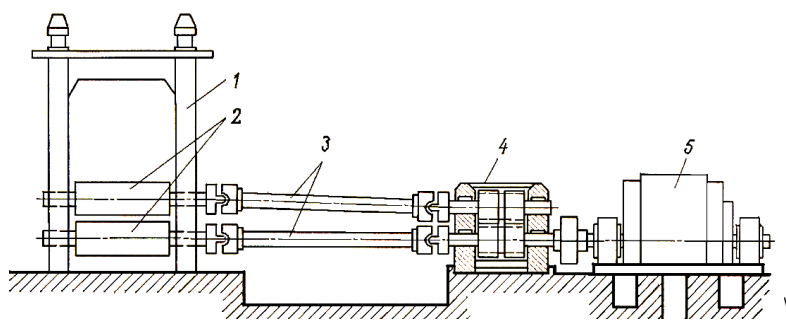
Прокатное производство Чусовского металлургического завода включает среднесортные станы «550» и «370», мелкосортные «250» и «200».

Среднесортный стан «370», состоящий из семи рабочих клеток, предназначен для производства рессорной полосы, а также спецпрофилей и профилей общего назначения.

Среднесортный стан «550», состоящий из трех рабочих клеток, производит среднесортной и фасонный прокат, ассортимент которого включает в себя сорок три наименования и используется в строительстве, машино- и автомобилестроении, судостроении, угольной промышленности.

Мелкосортные станы «250» и «200», состоящие из рабочих клеток, специализируются на производстве проката сортовых, фасонных профилей и профилей специального назначения, арматуры. Продукция стана применяется в автомобилестроении, машиностроении, строительстве и сельском хозяйстве.

За последующие годы на стане проведена существенная модернизация оборудования, замена рабочих клеток и изменение технологий. Проектная мощность его составляет 283,0 тыс. тонн проката в год. [2]



**Рисунок 1. Реверсивный стан с групповым приводом:** 1 – станина клетки; 2 – прокатные валки; 3 – универсальные шпиндели; 4 – шестеренная клетка; 5 – общий двигатель

По расположению рабочих клеток стан относится к станам линейного типа, состоит из двух рабочих трехвалковых клеток («трио»). Направление прокатки в линейно-расположенных клетках меняется. Валки подразделяются на рабочие, в которых происходит обжатие металла, и опорные. Рабочие валки являются приводными. Привод прокатных валков – групповой, при котором валки, установленные в станине клетки, приводятся во вращение от одного электродвигателя через шестеренную клетку и универсальные шпиндели. Клетки оборудованы подъемно-качающимися столами и кантователями. Специализация стана – заготовка квадратного и прямоугольного сечения размерами 99x99 мм – 110x110 мм, предназначенная для сортовых станов завода. Исходным продуктом служат слитки (слябы) своего завода и блюмы, поставляемые другими металлургическими предприятиями. Привод стана осуществляется от электродвигателя мощностью 3150 кВт через редуктор и шестеренную клетку.

Кроме прокатки металла на прокатном стане производится ряд вспомогательных операций: перемещение металла в продольном и поперечном направлениях относительно линии стана, подача металла к валкам, кантовка и резание металла, регулировка положения прокатных валков и т.д. Эти операции осуществляются с помощью вспомогательных механизмов стан, обеспечивающих определенную последовательность технологического процесса.

По назначению вспомогательные механизмы разделяют на транспортные, установочные, механизмы резания. К транспортным относятся механизмы перемещения и изменения положения металла. К установочным механизмам относятся нажимные устройства для установки верхнего валка, перевалки валков, перемещения клетей. К механизмам резания относятся ножницы поперечного и продольного резания, пилы и т.д.

Вспомогательные механизмы работают с продолжительным режимом нагрузки, механизмы с режимом кратковременной нагрузки, механизмы с режимом повторно-кратковременной нагрузки. [3]

Различают вспомогательные механизмы без регулирования скорости и механизмы с регулированием скорости.

Для привода механизмов, работающих в режиме продолжительной нагрузки, применяют асинхронные двигатели с короткозамкнутым ротором. Механизмы, работающие в режимах длительной или повторно-кратковременной нагрузки и требующие регулирования скорости, приводятся асинхронные двигатели или двигатели постоянного тока. Для механизмов, работающих в режиме повторно-кратковременной нагрузки и не требующих регулирования скорости, выбор типа двигателя определяется числом включений в один час привода механизма.

Вспомогательное оборудование – агрегаты и механизмы поточных технологических линий прокатных цехов подразделяют на две основные группы: транспортную, выполняющую операции по перемещению металла, подаче его к рабочим клетям и его кантовку и обрабатывающую, работа которой связана с операциями по отделке проката.

В настоящее время на обжимных станах приняты две схемы подачи слитков: челночная и кольцевая. На современных станах осуществляется кольцевая слиткоподача, дающая возможность обеспечить высокую его производительность, составляющую 5-6 млн. тонн и более в год годного проката. Кольцевая слиткоподача называется так потому, что движение слитковозов осуществляется по замкнутому кольцу. [4]

Для порезки готового проката на мерные длины и обрезки концов устанавливают ножницы для горячей и холодной резки с параллельными ножами. Ножницы могут иметь нижний или верхний рез. Ножницы с верхним резом имеют простую конструкцию. В процессе резания нижний нож неподвижен, а верхний, укрепленный в суппорте, с помощью гидравлического или кривошипного привода движется вниз и разрезает металл. Чтобы воспрепятствовать повороту полосы при резе, устанавливают специальный прижим, опускающийся на полосу с верхним ножом. Ножницы с нижним резом получили более широкое применение. Перед началом разрезания ножницы раскрыты и металл проходит между ними по рольгангу: нижний нож при этом находится ниже роликов рольганга и не мешает движению металла. Затем металл останавливается при помощи передвижного упора и суппорт верхнего ножа отпускается до соприкосновения с металлом. Дальнейшее продвижение верхнего суппорта прекращается и начинает двигаться суппорт нижнего ножа, при этом осуществляется резание металла.

Цикл работы реверсивной клетки стана горячей прокатки для одного пропуска в общем случае включает разгон валков вхолостую до скорости захвата слитка, разгон со слитком в валках до установившейся скорости, прокатку на этой скорости, торможение до скорости выброса слитка и реверс вхолостую до скорости захвата слитка, разгон со слитком в валках до установившейся скорости, прокатку на этой скорости, торможение до скорости выброса слитка и реверс вхолостую до скорости захвата при противоположном направлении вращения валков. Во время паузы между пропусками с помощью нажимного устройства клетки, приводимого от двигателей, производится перемещение верхнего прокатного валка для изменения раствора между валками в соответствии с требуемым обжатием. В случае необхо-

димости заготовка перемещается в поперечном направлении по рольгангу посредством линеек манипулятора и кантуется (поворачивается на 90° вокруг своей продольной оси) с помощью кантователя. Рабочий рольганг возвращает заготовку к клету для последующего пропуска. По окончании последнего пропуска заготовка транспортируется рольгангом к следующему механизму, а нажимное устройство перемещает верхний прокатный валок в первоначальное положение.

Печное хозяйство стана состоит из пяти методических нагревательных печей, четыре из которых однорядные двухзонные, пятая печь двухрядная трехзонная с рекуператором. Топливом для печей служит смесь природного и доменного газов и мазут. Печи оборудованы контрольно-измерительными приборами и тепловой автоматикой. В данный момент используются толкательная печь, которая имеет длинную прямоугольную камеру с форсунками, изделия на подходах или без них периодически проталкиваются по направляющим или роликам пода печи с помощью находящегося перед загрузочной дверцей механизма толкателя с электроприводом. На время проталкивания загрузочная и разгрузочная дверцы печи открываются. Достоинства толкательной печи в первую очередь определяется надежностью работы, поскольку механизм толкателя находится вне печи, а также возможностью обработки изделий большой массы. [5]

Слитки для посадки в печь укладываются на посадочный стол электромостовыми кранами грузоподъемностью пять тонн. Нагрев слитков в печах производится в соответствии с инструкцией по тепловому режиму. Нагретый слиток выдается с помощью пяти тележек в первую клету, где получается раскат, который поступает на вторую клету для окончательного формирования заготовки. Раскат поступает к ножницам горячей резки, где производится его порезка на полосы заданной длины. Заготовки маркируются, сдвигаются на стеллажи с помощью кантователей, охлаждаются, сортируются и мостовым краном с помощью специальных працер-захватов штабелируются в пролете адьюстажа. Оттуда заготовки двенадцатью вагонами местного парка транспортируются на станы «370», «550», «250». Отходы производства (обрезь) идет в мартеновские печи дуплекс цеха, окалина – на производство агломерата на аглофабрике. [6]

### Список литературы:

1. Акимова, Н.А. Монтаж, техническая эксплуатация и ремонт электрического и электромеханического оборудования – М.: Мастерство, 2002.
2. Мальцев, А.А. Индивидуальный электропривод прокатного стана / А.А. Мальцев // Перспективы науки. – 2017. – № 11(98). – С. 7-12. – EDN YNUIQC.
3. Кавалек, А. Исследование влияния режима листовой прокатки на качество полосы / А. Кавалек, Х. Дыя, К. Ожмегов // Черная металлургия. Бюллетень научно-технической и экономической информации. – 2020. – Т. 76, № 6. – С. 591-601. – DOI 10.32339/0135-5910-2020-6-591-601. – EDN SJABGY.
4. Воронцов Н.М. Периодические профили продольной прокатки, В.Т. Жадан, М.Ф. Грицук и др. М.: Металлургия, 1978. 232 с.
5. Федосов Н.М., Бринза В.Н., Астахов И.Г. Проектирование прокатных цехов. М.: Металлургия, 1983. 303 с.
6. Малафеев, С.И. Автоматизация технологического процесса прокатки специальных сплавов / С.И. Малафеев, А.А. Малафеева, В.И. Коняшин // Автоматизация в промышленности. – 2019. – № 1. – С. 15-18. – EDN VSXKVJ.



## АНАЛИЗ ПРОБЛЕМ ИСПОЛЬЗОВАНИЯ ОТЕЧЕСТВЕННЫХ СРЕДСТВ ПРОЕКТИРОВАНИЯ В СРЕДЕ ОБУЧЕНИЯ И ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

**Ковалев Кирилл Константинович**

студент,

Санкт-Петербургский

Морской Технический университет,

РФ, г. Санкт-Петербург

**Аннотация.** В рамках научной работы была поставлена задача проанализировать развитие событий на рынке профессионального программного обеспечения (ПО) для инженеров и конструкторов, а также разработать план перехода на отечественное программное обеспечение в связи с уходом многих иностранных компаний. После рассмотрения текущего состояния на рынке труда была выстроена необходимость в подборе аналогов на существующие позиции. Результатом является список программного обеспечения, которое отвечает всем требованиям, предъявляемым к приложениям, используемым в профессиональной деятельности как человека, так и компаний в целом.

### Введение

В последние два десятилетия происходит внедрение иностранной продукции в нашу жизнь. Теперь очень сложно представить, как обычный человек может не пользоваться телефоном и компьютером ежедневно.

И несмотря на то, что в последние 5 лет российские компании предпринимали попытки создать свои аналоги популярным и столь незаменимым смартфонам, они в большинстве своем оканчивались неудачами.

К сожалению, вскоре после неудач многие отделы отвечающие за разработку и создание этих устройств были закрыты.

Однако еще остались компании, которые работают над своими продуктами, с целью составить достойную конкуренцию в относительно недорогом сегменте рынка. Аппаратные составляющие это лишь часть взаимодействия между человеком и виртуальным миром.

Не менее важным, а за частую даже более важным элементом является программное обеспечение. Сложно найти такого человека, который не пользовался каким-либо приложением при использовании компьютера, смартфона.

Именно программы создают те эмоции и контент, к которому мы все привыкли за последние 20 лет.

Это является ключевым моментом в текущий момент реальности, поэтому в нынешних условиях уход многих иностранных компаний несет за собой экономические убытки, осложнение процессов глобализации или их полную остановку.

### Обзор состояния дел в предметной области

Многие отечественные компании не пытаются работать на перспективу и искать аналоги, чтобы подстраховаться и быть уверенными в будущем, и как следствие слабые шаги в сторону стабилизации своей деятельности и развитие пиратского контента.

Нередко выпускники сталкиваются с необходимостью умения работать в различных иностранных программах, или наличия опыта работы на данной должности. В основном, программы являются платными.

Иногда имеют бесплатную версию для студентов, однако ее действие имеет ограниченный период работы и для получения студенческой лицензии необходимо проходить специальную проверку раз в какой-то период. Также стоит отметить наличие пробного периода, обычно продолжительность составляет тридцать календарных дней.

К сожалению, это так же актуально для отечественного программного обеспечения, о котором сегодня пойдет речь.

Однако сегодня достаточно сложно найти вакансии требующие знаний в наших аналогах.

Зачастую, в списке требований, встречается такое программное обеспечение как: Autodesk 3ds max, Autodesk Maya, Autodesk AutoCAD, Autodesk Revit, SolidWorks. Эти компании остановили свою поддержку и обслуживание в России в начале 2022 года, что стало дополнительным препятствием в использовании программного обеспечения и обучении квалифицированных кадров, способных работать на разных платформах. Как следствие, нарушение стабильности в работе Российских компаний (различных архитектурных, конструкторских бюро) а также государственных учреждений (образовательные организации, промышленные предприятия и пр.).

Лицензионное программное обеспечение – это важная часть работы для многих компаний и архитектурных бюро. За использование пиратских версий на основании ст. 146 УК РФ «Нарушение авторских и смежных прав» [1] предусмотрено очень серьезное наказание: штраф до 200 000 Р за каждую пиратскую версию, лишение свободы до 2-х лет и конфискация оборудования (рабочих компьютеров). Использование пиратского программного обеспечения также отрезает архитекторов от сотрудничества с иностранными компаниями и от участия в госзаказах.

### **Постановка проблемы и методы ее решения**

Трудности с покупкой лицензии на программу могут поставить под вопрос существование бюро или компании, а перевод сотрудников на новые программные инструменты – это большие затраты, которые складываются не только из покупки новых программ, но и из обучения сотрудников, покупки нового оборудования, выстраивания новых рабочих процессов и времени, затраченного на адаптацию к ним. В текущих условиях, многие руководители находятся в растерянности.

Именно поэтому я поставил задачу проанализировать требования на рынке труда и найти отечественные аналоги наиболее востребованных программ.

Для этого необходимо проанализировать требования и составить перечень наиболее востребованных программ. Найти аналоги и оценить их на основе конкурента выявить преимущества и недостатки. Добавить в список конкурентно способных отечественных программ.

### **Решение поставленных задач**

Согласно данным, полученным с сервиса по поиску работы hh.ru (HeadHunter.ru), наиболее востребованными навыками являются умения работать в программах AutoCAD, ArchiCAD, Revit, 3dsMax, SolidWorks, Maya.

Теперь необходимо найти отечественные аналоги данным программам.

#### **1. nanoCAD**

Аналог программ: AutoCAD, ArchiCAD, Revit, Allplan, Tekla, Vectorworks;

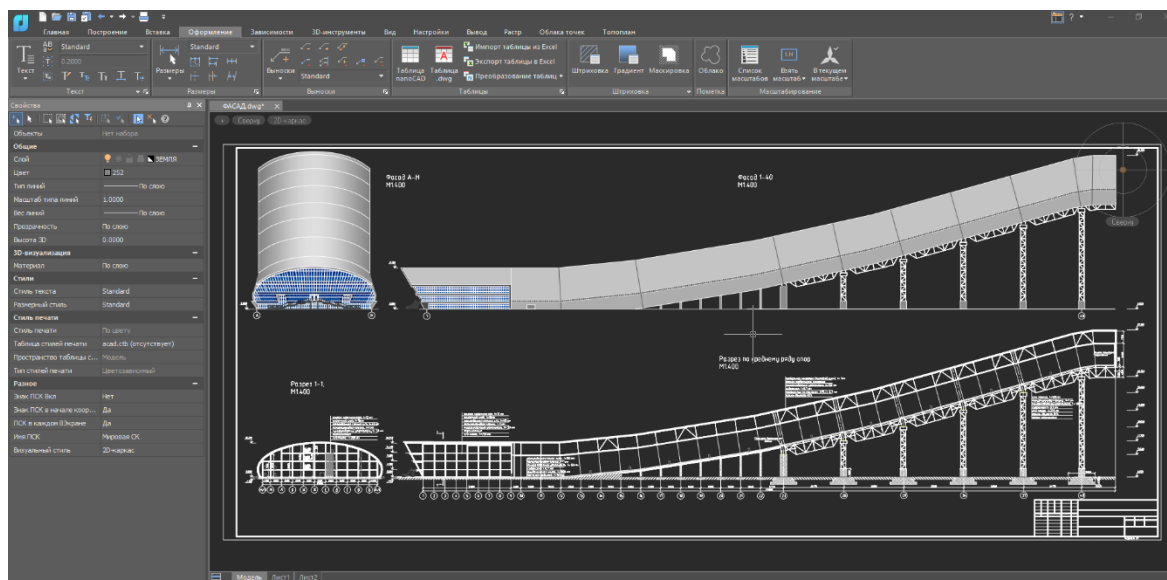
Операционная система: Windows;

Разработчик: Нанософт, Москва;

Стоимость: от 47 200 Р до 253 800 Р (на 25.05.2023), есть бесплатная версия для студентов;

Читаемые форматы файлов: DWG, DXF, DWT, SHP, C3B, STEP, DAE, PDF;

Создаваемые форматы файлов: DWG, DXF, SHP, PDF.



**Рисунок 1. Интерфейс программы nanoCAD**

nanoCAD – «это российская платформа для проектирования и моделирования объектов различной сложности. Поддержка форматов \*.dwg и IFC делает ее отличным решением для совмещения САПР- и BIM-технологий.» [1, с. 5] Функционал платформы может быть расширен с помощью специальных модулей.

Программы очень схожи по интерфейсу, инструментам и функциям. По словам разработчиков, программу специально сделали похожей на AutoCAD, чтобы упростить пользователям процесс перехода с одной программы на другую.

Главное отличие между программами – универсальность использования. У nanoCAD существует много форматов данного продукта специально разработанных для разных отделов проектной организации – от геодезистов до электриков. Так как программная платформа одинаковая, разные специалисты работают в одной среде, но при этом имеют инструменты необходимые именно для их специфики работы.

Также разработчик nanoCAD выпускает отдельные специализированные инструменты, предназначенные для облегчения взаимодействия разных отделов проектирования при работе над общей задачей – векторизация, создание архивов электронной документации, библиотеки нормативных документов. Этот подход помогает решить проблему совместимости программного обеспечения разных специалистов и лучше организовать BIM-процессы.

Однако назвать nanoCAD полноценным BIM-решением нельзя: классическая версия программы разработана для 2D-черчения, а существующие BIM-вариации nanoCAD сделаны для инженеров и конструкторов.

С точки зрения архитектора смоделировать здание как, например, в ArchiCAD, здесь нельзя. 3D-моделирование в nanoCAD такое же, как и в AutoCAD, то есть неполное, с ограниченным количеством инструментов и упрощенной визуальной составляющей.

## **2. КОМПАС-3D**

Аналог программ: AutoCAD, Inventor, SolidWorks;

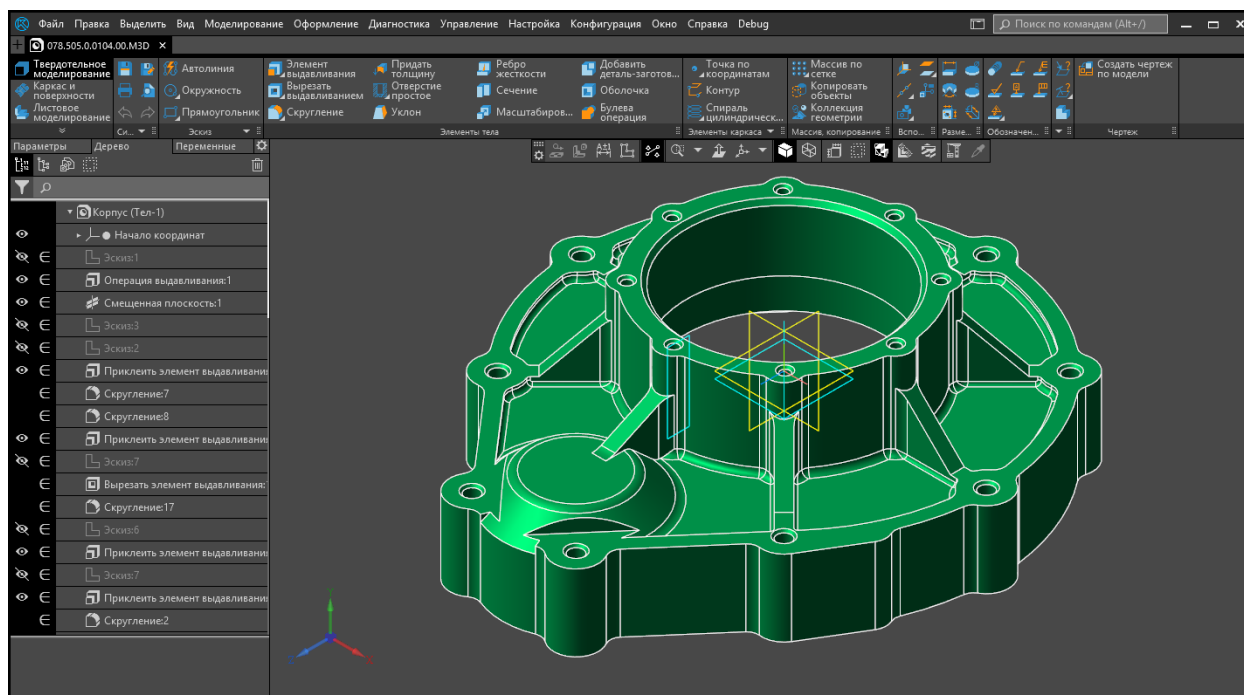
Операционная система: Windows;

Разработчик: Аскон, Санкт-Петербург;

Стоимость: от 1 490 ₽ до 195 000 ₽, есть бесплатная версия для студентов;

Читаемые форматы файлов: DWG, DXF, PDF, STEP, IGES;

Создаваемые форматы файлов: DWG, DXF, PDF, STEP, IGES, STL, C3D.



**Рисунок 2. Интерфейс программы КОМПАС-3D**

Программа КОМПАС-3D «предназначена для проектировщиков, конструкторов, инженеров, а так же для руководителей проектов в различных отраслях: промышленном и гражданском строительстве, энергетике, проектировании систем жизнеобеспечения и объектов инфраструктуры». [2, с. 6]

Гибкость настройки системы позволяет выполнить различные задачи пользователя, связанные с выпуском документации.

А поддержка распространенных форматов DXF/DWG дает возможность организовывать эффективный обмен данными с другими чертежно-графическими системами. КОМПАС 3D может подойти инженерам и конструкторам, так как обладает большой встроенной библиотекой технических деталей и материалов, а также содержит специальный модуль для анализа и расчёта смоделированных объектов.

Для архитекторов есть специальная версия КОМПАС-Строитель – классический САПР.

Программа не сильно отличается от AutoCAD или nanoCAD по инструментам и функциям 2D-черчения. Однако КОМПАС-Строитель не предназначен для 3D-моделирования, и не имеет BIM-функций. КОМПАС-3D свободно переносится в другие продукты разработчика – например, можно переносить 3D-модели в чертёжную среду, а затем выпускать альбом чертежей.

### **3. Renga**

Аналог программ: ArchiCAD, Revit, SketchUp, Allplan, Tekla, Vectorworks;

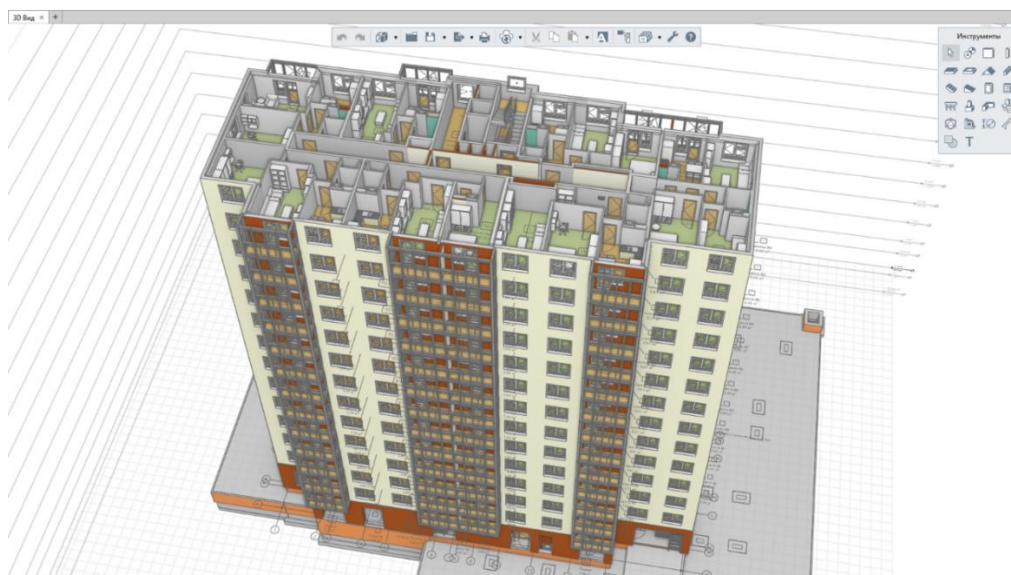
Операционная система: Windows;

Разработчик: Renga Software (Аскон + 1С), Санкт-Петербург;

Стоимость: от 5 000 Р до 110 000 Р, есть некоммерческая версия и версия для студентов;

Читаемые форматы файлов: IFC 4, IFC2x3, DWG, DXF, C3D, STEP, IGES, SAT, OBJ, DAE, PDF;

Создаваемые форматы файлов: RNP, RNT, DWG, DXF, PDF, STL, IFC.



**Рисунок 3. Интерфейс программы Renga**

«Renga – российская BIM-система для комплексного проектирования с необходимой функциональностью, интуитивно-понятным интерфейсом и доступной стоимостью. Вся документация, создаваемая в программе, соответствует используемой в России нормативно-технической документации. Созданная информационная модель объекта строительства используется на всем его жизненном цикле.» [3, с. 8]

Разработчики Renga позиционируют свой продукт как программное обеспечение, которое находится в стадии разработки, но регулярно обновляется. Программа действительно выглядит не готовой к массовому использованию. Главная особенность программы – проектирование ведётся только в 3D-виде, как в SketchUp. Основным недостатком программы является возможность использования только встроенные или сторонние модели, то есть отсутствует возможность создавать свои объекты.

Инструменты 2D-геометрии скудные – например, нет сопряжения, подрезки или удлинения линий.

Из плюсов можно отметить компактный и адаптивный интерфейс: под рукой только нужные настройки и функции, которые занимают небольшое пространство экрана. Также разработчики активно общаются с аудиторией и дорабатывают программу под условия реальной работы пользователей.

Renga сложно сравнивать с ArchiCAD или Revit с точки зрения проектирования, потому что в программе не хватает некоторых функций.

Однако по BIM-составляющей сравнить можно.

Разработчики выбрали путь Open BIM, а не создание собственных решений или партнёрство с другими компаниями. И этот путь неоднозначный. С одной стороны, с IFC-файлом можно работать во всех BIM-программах, а с другой, Renga поддерживает только старые форматы IFC, и они не очень удобны для работы конструктора или инженера.

При этом разработчики Renga параллельно развивают BIM-среду для архитекторов, инженеров и конструкторов.

Если программную среду доработают, то она имеет все шансы стать отличным инструментом.

Российские программы для черчения и моделирования ещё только на пути к тому, чтобы стать достойной альтернативой привычному, но покинувшему российский рынок программному обеспечению.

Есть отличные САПР-решения, которые большинству специалистов могут заменить AutoCAD. Но программы для моделирования не разработаны для работы над архитектурой.

Что касается инструментов для BIM-моделирования, то они ещё не готовы, чтобы полноценно заменить Revit или ArchiCAD. А то, что сейчас выдаётся за BIM-решения, фактически является продвинутым САПР.

### Результаты исследования

Результатом исследования является список программ способных конкурировать с иностранным программным обеспечением.

Правительство РФ издало указ о необходимости перехода на отечественное программное обеспечение, что привело к значительному усилению спроса на российские программные инструменты.

В связи с этим, отечественные разработчики захватывают рынок и устраивают собственные монополии в отсутствии западных конкурентов. Это приводит к случаям завышения цен, а также нежеланию идти на компромисс и доработку своего программного обеспечения до зарубежного уровня.

### Выводы по полученным результатам

Большинство российских программ страдают от своей безызвестности: их редко покупают, потому что о них мало кто знает.

В результате компании не обладают большими бюджетами на разработку – отсюда нехватка ряда функций и инструментов и устаревшие интерфейсы.

Сторонним разработчикам также невыгодно делать дополнительные инструменты и расширения для невостребованных программ.

В результате техническое отставание российского софта по сравнению с европейским и американским составляет 5–10 лет.

Обычно небольшие компании просто не могут состязаться с гигантами рынка, вроде Adobe или Autodesk, но если небольшая компания придумывает что-то новое в условиях жёсткой конкуренции, она превращается в известный бренд.

Отсутствие уникальности является второй проблемой российского программного инструментария.

Российские аналоги часто дублируют только часть инструментов известных программ и не предлагают ничего нового, и при этом могут стоить дороже.

Отставание отечественного программного обеспечения сократится, когда производители Российского ПО начнут разрабатывать новые инструменты и функции программ, а также развивать маркетинг.

Сейчас в России развивается BIM-область, но очень медленно.

Однако есть российские разработчики сред проектирования, которые неплохо удовлетворяют потребности профессионалов, оставаясь небольшими компаниями:

Renga откликается на запросы специалистов, а nanoCAD переманивает аудиторию за счёт более низких цен на лицензионное ПО.

Кроме российских разработчиков есть множество таких же небольших компаний по всему миру, которые предлагают больше возможностей.

А ещё есть открытый Open Source-программное обеспечение, которое предлагает схожие функции и вдобавок распространяется бесплатно.

Если российские компании не перестроятся быстро, освободившиеся места западных гигантов могут занять разработчики из Китая или других стран.

### Список литературы:

1. Официальный сайт продукта nanocad. URL:<http://www.nanocad.ru> (дата обращения 13.05.2023)
2. Официальный сайт продукта kompas. URL:<http://kompas.ru> (дата обращения 13.05.2023)
3. Официальный сайт продукта renga. URL:<http://rengabim.com> (дата обращения 13.05.2023)

# ПРОГРАММА АУДИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПУБЛИЧНЫХ ОБЛАКАХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ИХ ОБРАБОТКИ

**Кудряшов Дмитрий Петрович**

студент,

Московский институт электронной техники,

РФ, г. Москва

В результате исследования была разработана программа аудита информационной системы защиты персональных данных в публичных облаках. Она включает в себя следующие этапы:

- 1) Подготовка к аудиту, включающая определение целей, области аудита, критериев и методов аудита;
- 2) Оценка рисков безопасности информации в публичных облаках;
- 3) Анализ процессов обработки персональных данных в публичных облаках;
- 4) Анализ мер защиты информации в публичных облаках;
- 5) Оценка эффективности мер защиты информации в публичных облаках;
- 6) Подготовка отчета по результатам аудита.

## **1. Подготовка к аудиту, включающая определение целей, области аудита, критериев и методов аудита**

Пункт о деятельности по аудиту является основным в ISO 19011. Действия по аудиту также можно назвать этапами процесса или действиями. Аудиторская деятельность представляет собой пошаговые методы подготовки, проведения, отчетности и последующих действий по аудиту. Прежде чем приступить к аудиту системы или процесса, необходимо определить объем и критерии аудита [1].

ISO 19011, пункт 6.2.2 описывает объем аудита как объем и границы аудита. Это объясняется:

- 1) физическим местоположением (например, адресом, участком, этажом, площадью);
- 2) организационными единицами (например, отделом или филиалом);
- 3) деятельностью и процессами (такими как маркетинг, распиловка, андеррайтинг, линейка продуктов) и охватываемый период времени.

Как бы выглядело описание сферы деятельности вашей организации? Это помогает аудитору подготовиться и сохраняет его сосредоточенность. В общем, аудиторы должны всегда оставаться в рамках. Оставаться в пределах объема является хорошей практикой и позволяет избежать обвинений аудитора в охоте на ведьм. Однако в каких случаях аудиторам допустимо отклоняться от согласованного объема? Когда есть наблюдения, которые могут привести к возможным травмам, незаконным действиям, неэтичным действиям.

Определение критериев аудита является частью шага «что необходимо проверить». Критерий аудита означает все, что аудитор может проверить. Аудитор может проводить аудит в соответствии с любыми правилами, процедурами, задачами, задачами, контрактами, законами, кодексами поведения, передовой практикой и так далее [2].

Определение целей, объема и критериев аудита является ключом к определению всех оставшихся шагов процесса аудита для планирования, выполнения, отчетности и последующих действий. Этот шаг обеспечивает основу для индивидуального аудита. Плохая работа здесь напрямую повлияет на эффективность и результативность аудита.

## **2. Оценка рисков безопасности информации в публичных облаках**

Анализ мер защиты информации в публичных облаках в РФ проводится в соответствии с законодательством о защите персональных данных, включая Федеральный закон "О персо-



нальных данных" и Постановление Правительства РФ "О требованиях к защите персональных данных при их обработке в информационных системах персональных данных".

Шаг 1: Определение цели анализа. На этом этапе определяются цели и задачи анализа, какие меры защиты информации используются в публичном облаке и какие угрозы могут возникнуть при обработке персональных данных.

Шаг 2: Идентификация активов и уязвимостей. На этом этапе проводится анализ технологий, используемых в облаке, а также оцениваются уязвимости, которые могут быть использованы злоумышленниками для доступа к данным. Также проводится анализ технических средств защиты, используемых в облаке [3].

Шаг 3: Оценка соответствия требованиям законодательства. На этом этапе проводится анализ соответствия мер защиты информации требованиям законодательства о защите персональных данных, включая требования к согласованию обработки персональных данных с субъектами, правилам обработки персональных данных, а также требованиям к хранению и передаче персональных данных.

Шаг 4: Оценка вероятности возникновения угроз. На этом этапе проводится анализ возможных сценариев нарушения безопасности информации и определяются вероятности их возникновения, включая утечку данных в результате кибератаки, ошибки персонала или несанкционированный доступ [4].

Шаг 5: Оценка потенциальных последствий. На этом этапе оцениваются возможные последствия нарушения безопасности информации и потенциальный ущерб для клиентов и бизнес-процессов, включая финансовые потери, ущерб репутации и нарушение законодательства о защите персональных данных.

Шаг 6: Разработка мер по уменьшению рисков. На этом этапе разрабатываются меры по уменьшению рисков, связанных с обработкой информации в публичном облаке, включая использование шифрования данных, ограничение доступа к данным и регулярное обновление программного обеспечения.

Шаг 7: Оценка эффективности мер. На этом этапе оценивается эффективность принятых мер по уменьшению рисков безопасности информации в публичном облаке.

Шаг 8: Мониторинг и анализ. На последнем этапе происходит мониторинг безопасности информации в облаке и анализ эффективности принятых мер по ее защите. Если необходимо, проводится переоценка рисков и разработка дополнительных мер по уменьшению угроз [5].

### **3. Анализ процессов обработки персональных данных в публичных облаках**

Анализ процессов обработки персональных данных в публичных облаках включает оценку того, как провайдер облачных услуг обрабатывает и защищает персональные данные пользователей [6]. Это может включать следующие шаги:

1. Изучение политик и процедур провайдера облачных услуг в отношении обработки персональных данных. Это может включать анализ политик конфиденциальности, пользовательского соглашения и других документов, связанных с обработкой персональных данных;

2. Оценка процессов сбора, хранения и передачи персональных данных в публичных облаках. Это может включать проверку механизмов шифрования, анонимизации и других мер защиты данных;

3. Анализ процессов контроля доступа к персональным данным в публичных облаках. Это может включать проверку механизмов аутентификации, авторизации и аудита доступа;

4. Оценка мер безопасности провайдера облачных услуг, связанных с обработкой персональных данных. Это может включать проверку мер защиты от угроз безопасности, таких как вредоносное ПО, фишинг-атаки и другие виды киберпреступности;

5. Анализ процедур управления рисками в отношении обработки персональных данных в публичных облаках. Это может включать проверку процедур резервного копирования данных, восстановления после сбоев и других мер по обеспечению непрерывности бизнеса [7];

6. Оценка соответствия провайдера облачных услуг требованиям законодательства в отношении защиты персональных данных. Это может включать проверку соответствия Общему регламенту о защите персональных данных (GDPR) или другим законодательным актам.

Проведение анализа процессов обработки персональных данных в публичных облаках может быть выполнено специалистами по информационной безопасности, используя различные инструменты и методы аудита. Результаты анализа могут быть использованы для определения рисков безопасности и разработки рекомендаций по улучшению процессов обработки персональных данных в публичных облаках [8].

#### **4. Анализ мер защиты информации в публичных облаках**

Для защиты информации от угроз провайдеров облачных услуг применяются различные технические и организационные меры, которые включают:

1) Шифрование данных: для защиты персональных данных пользователей провайдер облачных услуг может использовать механизмы шифрования данных. Это позволяет защитить данные от несанкционированного доступа и утечек;

2) Анонимизация данных: Анонимизация данных позволяет скрыть личную информацию пользователя, что делает ее невозможной для идентификации. Это может быть полезным, когда пользователь не хочет раскрывать свою личную информацию;

3) Согласованность с законодательством: Провайдер облачных услуг должен следить за соответствием обработки персональных данных законодательству о защите персональных данных, чтобы предотвратить возможные нарушения;

4) Прозрачность в отношении обработки данных: Провайдер облачных услуг должен предоставлять пользователям информацию о том, как их данные используются. Это позволяет пользователям принимать более осознанные решения о предоставлении своих данных;

5) Ограничение доступа: Провайдер облачных услуг должен ограничить доступ к персональным данным только тем сотрудникам, которые имеют необходимость в их обработке;

6) Аудит процессов обработки данных: Регулярный аудит процессов обработки персональных данных помогает обнаружить и устранить возможные нарушения безопасности;

7) Защита от утечек: для защиты от утечек провайдер облачных услуг может использовать механизмы контроля доступа и политики безопасности;

8) Возможность удаления данных: Провайдер облачных услуг должен предоставить возможность удаления персональных данных пользователей при необходимости.

#### **5. Оценка эффективности мер защиты информации в публичных облаках**

Оценка эффективности мер защиты информации в публичных облаках может быть сложной задачей, поскольку она зависит от многих факторов, включая тип данных, тип приложений, методы шифрования и доступа, а также уровень требований к безопасности. Однако, провайдеры облачных услуг должны следить за тем, чтобы их меры защиты соответствовали самым высоким стандартам безопасности и отвечали требованиям законодательства.

Шифрование данных является одним из наиболее эффективных способов защиты информации в публичных облаках [9]. Хорошо спроектированная система шифрования может предотвратить несанкционированный доступ к данным и уменьшить риск утечки информации. Однако, провайдеры облачных услуг также должны следить за тем, чтобы процесс шифрования был прозрачным для пользователей и не замедлял производительность приложений.

Анонимизация данных также может быть полезной мерой защиты информации в публичных облаках. Это может помочь предотвратить идентификацию пользователей по их личной информации, что может быть особенно важным для организаций, которые обрабатывают чувствительные данные [7].

Ограничение доступа к персональным данным только тем сотрудникам, которые имеют необходимость в их обработке, также является важной мерой защиты информации. Это может помочь предотвратить случайные или злонамеренные утечки данных [10].

В целом, меры защиты информации, применяемые провайдерами облачных услуг, могут быть эффективными в предотвращении угроз безопасности. Однако, для обеспечения

максимальной защиты, необходимо обеспечить соответствие мер безопасности требованиям законодательства и наилучшим практикам безопасности. Также следует регулярно аудиторировать процессы обработки персональных данных и обновлять меры защиты в соответствии с изменяющейся угрозой безопасности.

## **6. Подготовка отчета по результатам аудита персональных данных в публичных облаках**

Отчет по результатам аудита персональных данных в публичных облаках должен включать следующие разделы:

1) Введение. В этом разделе должны быть описаны цели и задачи аудита, а также область его проведения;

2) Описание публичных облаков, которые были проанализированы. В этом разделе нужно представить общую информацию о каждом из облаков, включая провайдера, тип услуги, уровень безопасности и т.д.;

3) Анализ мер защиты информации, применяемых в каждом из публичных облаков. В этом разделе должны быть описаны меры защиты, применяемые провайдерами облачных услуг, такие как шифрование данных, анонимизация данных, ограничение доступа и т.д. Каждая мера должна быть оценена на эффективность и соответствие требованиям законодательства и наилучшим практикам безопасности;

4) Анализ рисков безопасности данных. В этом разделе необходимо описать выявленные уязвимости и угрозы безопасности данных в каждом из публичных облаков, а также оценить их вероятность и возможные последствия;

5) Рекомендации по улучшению мер защиты информации. В этом разделе должны быть предложены конкретные меры по улучшению безопасности данных в каждом из публичных облаков на основе выявленных уязвимостей и угроз безопасности;

6) Заключение. В этом разделе нужно подвести итоги аудита и оценить эффективность мер защиты информации в публичных облаках.

### **Список литературы:**

1. Дроздова, И.И. Безопасность облачных хранилищ / И.И. Дроздова, В.В. Жилин. – Текст : непосредственный // Технические науки в России и за рубежом : материалы VII Междунар. науч. конф. (г. Москва, ноябрь 2017 г.). – Москва : Буки-Веди, 2017. – С. 16-18. [Электронный ресурс]. – URL: <https://moluch.ru/conf/tech/archive/286/13236/> (дата обращения: 27.02.2023).
2. Международные стандарты аудита : учебное пособие для магистратуры / Л.Л. Арзуманова, Н.Ю. Орлова, О.С. Соболев, Ю.К. Цареградская ; отв. ред. Л.Л. Арзуманова, Ю.К. Цареградская. – Москва : Норма : ИНФРА-М, 2021. – 152 с.
3. Методика аудиторской проверки: процедуры, советы, рекомендации : монография / Д.Ю. Самыгин, Н.Г. Барышников, А.А. Тусков [и др.] ; под ред. Н.Г. Барышникова. – Москва : ИНФРА-М, 2020. – 231 с.
4. Парушина, Н.В. Аудит: практикум : учебное пособие / Н.В. Парушина, С.П. Суворова, Е.В. Галкина. – 3-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2020. – 286 с.
5. Преимущества облачных вычислений. – Текст : электронный // Microsoft: [Электронный ресурс] – URL: <https://www.microsoft.com/ru-ru/windows-365/cloud-computing-advantages> (дата обращения: 07.02.2023).
6. Приказ ФСТЭК "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 18.02.2013 № 21 (дата обращения: 01.03.2023).

7. Самые безопасные облачные хранилища 2020 // Falcongaze [Электронный ресурс]. Режим доступа: <https://falcongaze.com/ru/pressroom/publications/articles/safest-cloud-storage-2020.html> (дата обращения: 01.03.2023).
8. Фокин Н.Б., статья Обоснование эффективности использования Облачных технологий «Режим доступа – свободный. URL: <http://journal.itmane.ru/node/649> (дата обращения: 20.10.2019).
9. Joy A.M. Performance comparison between linux containers and virtual machines // Intl. Conf. on Advances in Computer Engineering and Applications. – Ghaziabad, India: IEEE, 2015.– С. 342–346. [Электронный ресурс] Режим доступа: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7164727&isnumber=7164643> (дата обращения: 04.03.2023).
10. Lombardi, F., Di Pietro Secure virtualization for cloud computing // J. Netw. Comput. Appl. – 2010. – №34(4). – С. 13–1122 (дата обращения: 04.03.2023).

## ОЦЕНКА РЕЗУЛЬТАТИВНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

*Майоров Марсель Сергеевич*

*магистрант,  
Казанский Национальный Исследовательский  
Технологический Университет,  
РФ, г. Казань*

Одной из главных обязанностей компании, сертифицированной на соответствие международным и национальным стандартам, является компетентная оценка эффективности применяемой системы управления качеством. Оценка системы менеджмента качества (СМК) – процесс, позволяющий оценить соответствие системы менеджмента качества необходимым требованиям и стандартам. Оценка проводится с целью определения эффективности системы в плане достижения поставленных перед системой менеджмента целей и задач, а также с целью выявить возможные улучшения и корректировки [1].

Оценка результативности системы менеджмента качества может проводиться по различным критериям, в зависимости от целей организации и выбранной методики оценки. Одним из основных критериев является удовлетворенность клиентов продукцией или услугами компании [2]. Для оценки этого критерия используются различные методы, такие как опросы клиентов, анализ рекламаций и жалоб, мониторинг рынка и т.д.

Еще одним важным критерием является эффективность работы системы менеджмента качества, которая может быть измерена по результатам аудитов, оценке эффективности процессов, улучшению показателей производительности и другим подобным показателями.

Так же можно проводить оценку результативности системы менеджмента качества с точки зрения ее соответствия стандартам и требованиям законодательства. Для этого проводятся проверки соответствия стандартам ISO, аудиты соответствия законодательным требованиям и т.д.

Все вышеперечисленные критерии могут использоваться в различных комбинациях для оценки результативности системы менеджмента качества и определения областей, требующих улучшения [3].

Оценка текущего состояния системы менеджмента качества в организации АО «Внебо-сервис» проводится путем проведения внутренних аудиторских проверок, анализа документации и записей. Анализ проводится начальником СК – главным контролером с периодичностью один раз в год на основании входных данных, предоставляемых структурными подразделениями и должностными лицами организации. Отчет содержит обоснованный вывод о соответствии СМК заявленной политике организации в области качества. Отчет содержит вывод и рекомендации по улучшению системы менеджмента качества.

Расчет результативности СМК включает следующие этапы: определение показателей частных критериев результативности СМК, определение частных критериев результативности, определение результативности СМК; интерпретация оценки результативности СМК организации.

Результативность СМК определяется как средневзвешенное значение шести частных критериев результативности, согласно требований ГОСТ Р ИСО 9001. Частные критерии имеют свой весовой коэффициент (b). Частные критерии с весом коэффициента равный 1 характеризуют: удовлетворенность потребителей качеством выпускаемой предприятием продукции, соответствие продукции требованиям. Частные критерии с весом коэффициента равный 0,9 характеризуют: степень выполнения требований ГОСТ Р ИСО 9001, зависящих от вида деятельности организации, степень выполнения установленных критериев результативности процессов. Частные критерии с весом коэффициента равный 0,8 характеризуют: реализацию политики в области качества и степень выполнения целей в области качества.

Значение удовлетворенности потребителей качеством выпускаемой предприятием продукции определяется как средневзвешенная оценка показателей: доля продукции, сданной с первого предъявления заказчику с весом 0,9, доля продукции, на которую не получены ре-

кламации, в общем числе сданной продукции с весом 0,9, доля продукции, на которую от заказчика не получены несоответствия, не оформленные в виде рекламаций, но признанные организацией, в общем числе сданной продукции с весом 0,7.

Значение соответствие продукции требованиям определяется как средневзвешенная оценка показателей: доля продукции, не забракованной СК при операционном контроле с весом 0,8, доля продукции, сданной с первого предъявления СК с весом 0,8, доля продукции, принятой без отклонений по согласованию с заказчиком с весом 1, доля неповторяющихся несоответствий продукции по данным из записей с весом 1.

Значение степень выполнения требований ГОСТ Р ИСО 9001, зависящих от вида деятельности организации определяется как средневзвешенная оценка показателей: доля специальных и особо ответственных технологических процессов, имеющих свидетельства аттестации, доля технологических операций без нарушения технологической дисциплины от проверенных технологических операций, доля измерительного, контрольного и испытательного оборудования, прошедшего поверку и аттестацию в запланированные сроки, доля продукции, выпущенной и принятой в соответствии с производственным планом, доля персонала, прошедшего обучение и аттестацию в соответствии с установленными требованиями с весом всех критериев 1.

Значение степень выполнения установленных критериев результативности процессов определяется как среднее из показателей: выполнение контрактов в установленный срок – отношение количества выполненных контрактов по отношению к общему количеству контрактов за анализируемый период, соответствие закупленной продукции сопроводительной документации – отношение объема закупленной продукции, соответствующей документации, к общему объему проверенной (в шт.), выполнение производственной программы в установленные сроки – отношение объема произведенной продукции к запланированному уровню по программе (плану) выпуска (ремонта), уровень технологической дисциплины – отношение количества операций без нарушения технологической дисциплины к общему количеству проверенных, выполнение обязательств по срокам – отношение количества случаев своевременного ремонта гарантийных изделий к суммарному объему работ, процент реализованных пунктов мероприятий по качеству – отношение выполненных пунктов мероприятий к общему их количеству, реализация графиков аудитов – отношение количества выполненных к общему количеству запланированных, доля выполненных пунктов планов по подготовке персонала – отношение количества выполненных пунктов к общему количеству пунктов, своевременное обеспечение и корректировка СТО – отношение количества разработанных (переработанных) документов к общему количеству запланированных, реализация графиков поверки, калибровки, аттестации – отношение количества выполненных пунктов к общему количеству.

Значение качество продукции поставщиков определяется по отношению количества годной продукции поставщиков к общему количеству поставленной продукции.

Значение реализации политики в области качества и степень выполнения целей в области качества определяется по отношению количества выполненных к общему количеству установленных целей.

Интерпретация полученных значений приведена в таблице 1.

**Таблица 1.**

### Результативность СМК

Полученная оценка результативности СМК	Результативность СМК
$R_{смк} < 0,60$	недопустимая
$0,60 < R_{смк} < 0,80$	допустимая
$0,80 < R_{смк} < 0,95$	достаточная
$R_{смк} > 0,95$	высокая

По результатам оценки оформляется отчет, который может представляться в орган по сертификации СМК в составе исходных материалов, направляемых вместе с заявкой на сертификацию (инспекционный контроль) СМК.

По итогам аудитов организуются мероприятия по устранению несоответствий, выявленных в процессе аудита. После этого проверяются эффективность корректирующих действий. Используется методика PDCA («планируй, выполняй, контролируй, действуй»), которая позволяет поэтапно улучшать процессы системы менеджмента качества на предприятии.

**Список литературы:**

1. Ермольева, М. Д. Возможности системы менеджмента качества на малых предприятиях-распространенные подходы и проблемы внедрения / М. Д. Ермольева // Аллея науки. – 2019. – Т. 1, № 1(28). – С. 394-397.
2. Кучерявенко, С.А. Развитие системы менеджмента качества – конкурентное преимущество образовательных организаций / С. А. Кучерявенко // Экономика. Информатика. – 2022. – Т. 49, № 2. – С. 277-284.
3. ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования: дата введения 2015-11-01. – Москва: Стандартиформ, 2015. – 23 с.

## ТИРАТРОН

### **Павлов Вадим Алексеевич**

студент,  
Улан-Удэнского колледжа железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

### **Разумов Данил Владимирович**

студент,  
Улан-Удэнского колледжа железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

### **Агунов Эрдем Александрович**

студент,  
Улан-Удэнского колледжа железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

### **Павлова Светлана Валерьевна**

научный руководитель,  
Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

Цель исследования: изучить тиратрон.

Задачи исследования: изучить устройство, работу и применение тиратрона.

### **Актуальность**

Тиратроном называют газоразрядный прибор, который имеет один или несколько дополнительных электродов-сеток. Водородные тиратроны относятся к типу тиратронов с накаливаемым катодом, который обычно является оксидным катодом косвенного накала. Тиратроны с накаливаемым катодом применяются в качестве мощных газоразрядных управляемых приборов, которые выполняют функцию выпрямления и преобразования переменного тока промышленной частоты 50 Гц. Они также используются в электроприводах, релаксационных схемах, релейных, инверторных, контролирующих, защитных и сварочных устройствах. Мощный тиратрон с накаливаемым катодом имеет анод, катод и сетку, которая управляет зажиганием. Баллоны тиратронов наполняются инертными газами, ртутными парами или водородом в зависимости от типа прибора.

### **Принцип работы**

Тиратрон – это газоразрядный прибор с одним или несколькими дополнительными электродами-сетками, который используется для выпрямления и преобразования переменного тока промышленной частоты. В тиратроне возникает разряд на анод благодаря уменьшению отрицательного смещения на сетке. При этом электроны начинают проникать в пространство между сеткой и анодом, ионизируя газ. В результате образуется плазма, которая обладает высокой проводимостью и отпирает тиратрон. Тиратроны с накаливаемым катодом применяются в различных устройствах, таких как электроприводы, сварочные и защитные устройства.

Первая характеристика – возможность формирования плазмы внутри прибора, что обеспечивает его работу в качестве выпрямителя и преобразователя переменного тока. Вторая характеристика – способность быстро восстанавливать управляющие свойства сетки после выключения прибора, что позволяет использовать тиратроны в различных устройствах, где



требуется точное управление электрическим током. Кроме того, важно отметить, что при выключении тиратрона происходит постепенный распад плазмы, что позволяет избежать повреждения прибора и обеспечивает его долговечность.

### **Технические характеристики**

Первая характеристика тиратронов с газовым наполнением заключается в возможности формирования плазмы внутри прибора, что позволяет использовать его в качестве выпрямителя и преобразователя переменного тока. Кроме того, такие тиратроны обладают способностью быстро восстанавливать управляющие свойства сетки после выключения прибора, что делает их полезными в различных устройствах, требующих точного управления электрическим током. Одним из главных преимуществ тиратронов с газовым наполнением является их малая зависимость от температуры окружающей среды. Это отличает их от ртутных тиратронов, для которых внешняя температура должна быть ограничена определенными пределами. Превышение этой температуры может привести к росту давления и понижению пробивной прочности, а при температурах ниже допустимой затрудняется возникновение разряда. Кроме того, тиратроны с газовым наполнением не требуют восстановительного разогрева для разложения амальгамы бария, как это необходимо для ртутных тиратронов. Такой процесс может занимать от 0,5 до 2 часов в зависимости от мощности прибора. В целом, тиратроны с газовым наполнением обладают рядом преимуществ перед ртутными тиратронами, что делает их более универсальными и надежными в использовании.

### **Особенности работы**

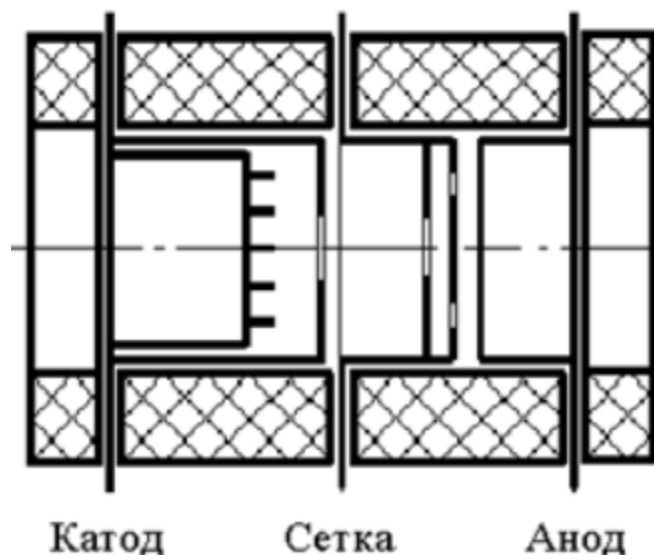
Первое преимущество тиратронов с газовым наполнением заключается в возможности формирования плазмы внутри прибора, что позволяет использовать его в качестве выпрямителя и преобразователя переменного тока. Также такие тиратроны быстро восстанавливают управляющие свойства сетки после выключения прибора, что делает их полезными в различных устройствах, требующих точного управления электрическим током. Одним из главных преимуществ тиратронов с газовым наполнением является их малая зависимость от температуры окружающей среды.

Это отличает их от ртутных тиратронов, для которых внешняя температура должна быть ограничена определенными пределами. Превышение этой температуры может привести к росту давления и понижению пробивной прочности, а при температурах ниже допустимой затрудняется возникновение разряда.

Тиратроны с газовым наполнением не требуют восстановительного разогрева для разложения амальгамы бария, как это необходимо для ртутных тиратронов. Такой процесс может занимать от 0,5 до 2 часов в зависимости от мощности прибора. Тиратроны с водородным наполнением обладают высокой скоростью деионизации, что обеспечивает минимальное время возникновения разряда тиратрона при импульсной работе. Кроме того, высокое значение катодного потенциала водорода позволяет использовать его без опасности разрушения оксидного катода. Некоторые импульсные тиратроны могут быть наполнены инертными газами.

Однако тиратроны с водородным наполнением имеют жестчеющий эффект на водород, что может изменять пусковые характеристики прибора.

Поэтому в качестве электродов водородных приборов используется высококачественный электролитический никель, свободный от вредных примесей, а мощные импульсные тиратроны могут быть оснащены генератором водорода для поддержания давления в колбе неизменным в течение всего срока службы.



*Рисунок 1. Схематичное конструкция тиратрона*

### Заключение

Хотя на сегодняшний день тиратроны и не пользуются большой популярностью из-за появления тиристоров, обладающих присущими им достоинствами, наличие такого типа тиратронов, как импульсные водородные тиратроны все ещё позволяет им конкурировать в некоторых областях науки и техники.

Они не сильно зависят от изменения температуры окружающей среды (по сравнению с ртутными тиратронами), позволяют переключать большие импульсные токи и напряжения, а также обладают большим быстродействием по сравнению с тиратронами. В качестве импульсных коммутаторов тока водородные импульсные тиратроны находятся вне конкуренции.

### Список литературы:

1. Сайт «Музей электронных раритетов» [www.1551a3.ru](http://www.1551a3.ru) // Раздел «Пассив» // Раздел «Электрoвакуумные приборы» // Статья «Тиратроны с накаливаемым катодом»
2. Сайт «Большая Энциклопедия Нефти и Газа» [www.ngpedia.ru](http://www.ngpedia.ru) // Статья «Водородные тиратроны»
3. Сайт «Электронная библиотека» [www.ntlib.chat.ru](http://www.ntlib.chat.ru) // Раздел «Электронные лампы» // Статья «Тиратроны»

## ВЛИЯНИЕ ТЕМПЕРАТУРНОГО РЕЖИМА ПОЖАРА НА ОГНЕСТОЙКОСТЬ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ

**Рыжова Мария Николаевна**

магистрант,  
Поволжский государственный  
технологический университет,  
РФ, г. Йошкар-Ола

**Смотрин Константин Александрович**

научный руководитель, канд. техн. наук,  
доцент, Поволжский государственный  
технологический университет,  
РФ, г. Йошкар-Ола

## INFLUENCE OF FIRE TEMPERATURE CONDITIONS ON THE FIRE RESISTANCE OF BUILDING STRUCTURES

**Maria Ryzhova**

Undergraduate, Volga State  
University of Technology,  
Russia, Yoshkar-Ola

**Konstantin Smotrin**

Scientific adviser, candidate of technical sciences,  
Associate Professor, Volga State University of Technology,  
Russia, Yoshkar-Ola

**Аннотация.** В работе изучены различные факторы, влияющие на температурный режим пожара и огнестойкость строительных конструкций. Определено, что температурный режим реального пожара отличен от стандартного. Предел огнестойкости в условиях реального пожара может наступить раньше времени, полученного при стандартном испытании.

**Abstract.** In this paper various factors affecting the temperature regime of a fire and the fire resistance of building structures have been studied. It is determined that the temperature regime of a real fire is different from that of a standard fire. The fire resistance limit in a real fire may come before the time obtained in a standard test.

**Ключевые слова:** огнестойкость, температурный режим пожара, строительные конструкции.

**Keywords:** fire resistance, fire temperature regime, building structures.

Огнестойкость строительных конструкций является немаловажным критерием для обеспечения пожарной безопасности. Она позволяет оценить способность конструкции сопротивляться воздействию пожара. Огнестойкость – способность строительной конструкции сохранять несущие и (или) ограждающие функции в условиях пожара [4]. В числовом выражении огнестойкость определяется её пределом, который устанавливается временным промежутком от начала огневого воздействия до проявления предельных состояний, измеряемым в минутах.

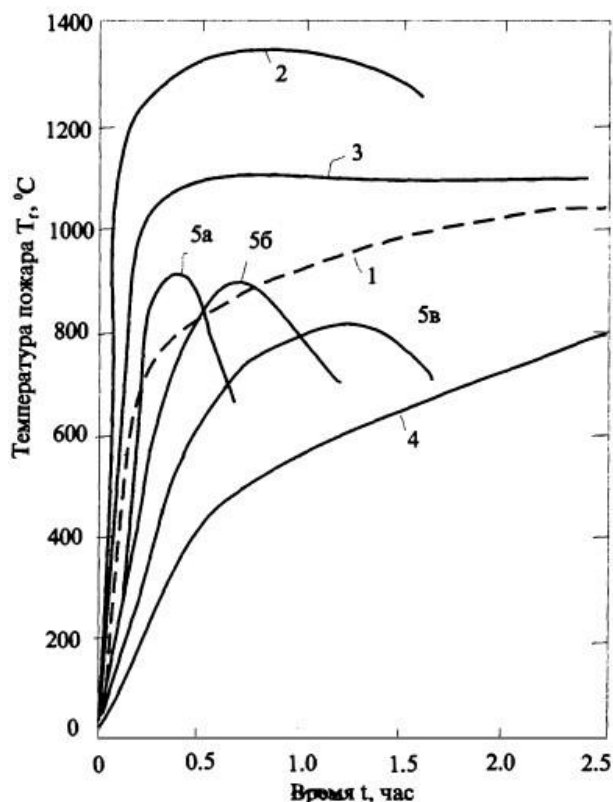
В целях определения фактического предела огнестойкости, которым должна обладать строительная конструкция, проводят экспериментальные исследования и расчеты. Чаще всего при их выполнении за основу берется стандартный температурный режим пожара. Следует отметить, что, проводя испытания и расчеты, основанные на стандартном температурном

режиме, не учитывается влияние данного режима как фактора, оказывающего воздействие на огнестойкость конструкции.

Температурный режим пожара – это изменение среднеобъемной температуры среды при пожаре в зависимости от времени его развития [3].

В настоящее время существует множество зданий и сооружений различного назначения, и их температурные режимы в значительной мере отличаются друг от друга. Ройтман В.М. графически выразил развитие среднеобъемной температуры во времени для отличных друг от друга зданий и сооружений. Данные графики представлены на рисунке 1.

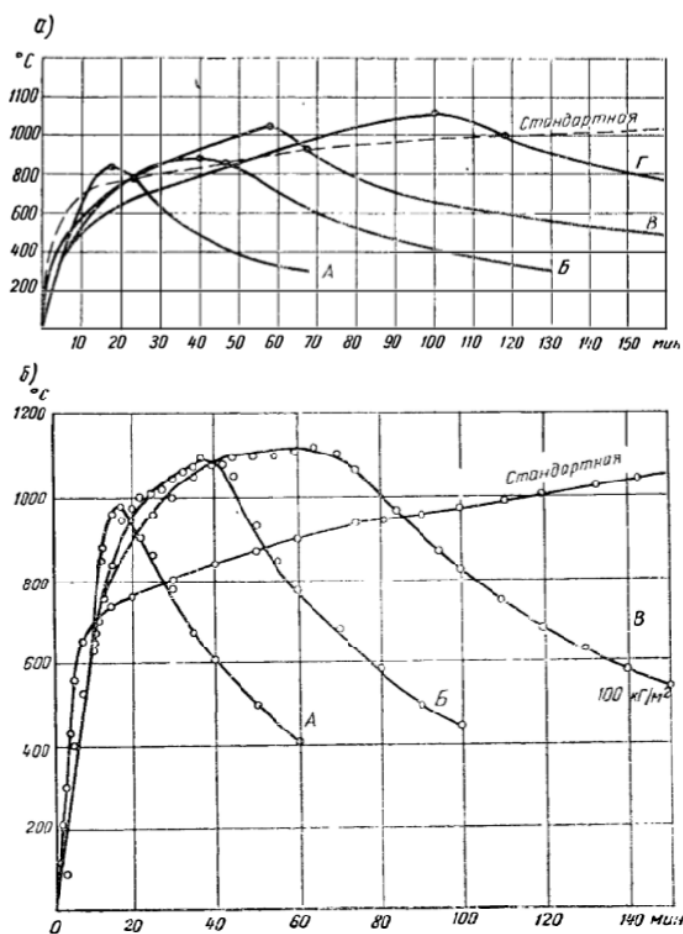
Взглянув на рисунок 1, видим, что в некоторых случаях за короткий промежуток времени температура пожара достигает значений больших, чем при стандартных испытаниях. Следовательно, фактический предел огнестойкости, полученный во время испытаний или расчетов, в основе которых лежит стандартный температурный режим, не предусматривает более высокотемпературного воздействия. Исходя из этого, конструкция достигает свой предел огнестойкости за меньший временной промежуток, чем при стандартном испытании. В другом случае, например, при пожаре в подвальных помещениях среднеобъемная температура ниже, чем у стандартного режима пожара, ввиду недостатка кислорода, необходимого для развития горения. В данном случае фактический предел огнестойкости, полученный при стандартном испытании, обеспечит выполнение основных функций строительных конструкции в условиях пожара, но с точки зрения экономической выгоды можно было бы использовать конструкции с меньшим пределом огнестойкости.



**Рисунок 1. Температурные режимы пожаров в помещениях зданий и сооружений различного назначения [3]: 1 – режим стандартного пожара; 2 – режим пожара в туннелях; 3 – режим пожара, характерный для зданий и сооружений нефтеперерабатывающей и нефтехимической промышленности; 4 – режим пожара в подвальном помещении; 5 – режим пожара в опытном помещении (типа жилого) с различной площадью проемов**

На температурный режим пожара, помимо геометрии помещения, влияет и горючее вещество, участвующее в пожаре. На рисунке 1 это доказывает кривая 3. В данном источни-

ке [3] описана зависимость температурного режима пожара от удельного количества сгораемых материалов, она представлена на рисунке 2.



**Рисунок 2. Температурные кривые, полученные при сжигании:** а) древесины в количестве 25, 50, 100 и 150 кг/м<sup>3</sup> (кривые А, Б, В и Г соответственно); б) автомобильных шин (кривые А, Б и В соответственно) [2]

Из кривых, изображенных выше, видим, что с увеличением удельного количества горючих материалов временные рамки действия пожара расширяются, а также возрастает максимальная температура, наблюдаемая в помещении при пожаре.

В результате пожара величина нанесенного строительной конструкции урона имеет зависимость не только от максимальной температуры огневого воздействия, но и от его продолжительности, учитывая стадии развития и затухания. Короткий временной промежуток стадии развития пожара способствует тому, что строительная конструкция может не прогреться до критических температур, при которых она достигнет своего предела огнестойкости. Увеличение данного временного интервала приводит к наступлению предельных состояний, и конструкция перестает удовлетворять требования безопасности. Стоит отметить, что помимо стадии развития пожара, на поведение строительных конструкций влияет и стадия затухания. В некоторых случаях на данной стадии железобетонные конструкции перестают выполнять свои функциональные требования и исчерпывают свой предел огнестойкости.

Температурный режим реального пожара может иметь значительные отличия от стандартного. В связи с чем наблюдается потребность в оценке огнестойкости строительных конструкций в реальных условиях.

Стандартная кривая температура-время была принята в 1959 году и используется до сих пор. Данная кривая не отражает влияния геометрии реального помещения и его пожарной нагрузки, а также никак не учитывает скорость изменения температуры реального пожара.

Требуемые пределы огнестойкости, изложенные в нормативных документах, определялись опытным путем и лишь косвенно учитывают факторы, влияющие на температурный режим пожара. Исходя из этого, опять же возникает потребность в оценке огнестойкости в условиях реального пожара.

**Список литературы:**

1. ГОСТ 30247.0-94 (ИСО 834-75) Конструкции строительные. Методы испытаний на огнестойкость. Общие требования : дата введения 01.01.1996. – Москва : ИПК Издательство стандартов, 2003. – 11 с.
2. Огнестойкость зданий / В.П. Бушев [и др.]; под общ. ред. В.А. Пчелинцева. – 2-е изд. – М.: Издательство литературы по строительству, 1970. – 261 с.
3. Ройтман, В.М. Инженерные решения по оценке огнестойкости проектируемых и реконструируемых зданий / В.М. Ройтман. – Москва : Пожарная безопасность и наука, 2001. – 382 с.
4. СП 2.13130.2020 СИСТЕМЫ ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ : дата введения 2020-09-12. – Москва : Стандартиформ, 2020. – 42 с. – URL: <https://docs.cntd.ru/document/565248963> (дата обращения: 08.05.2023). Текст: электронный

## ГИДРОЭЛЕКТРОСТАНЦИИ

**Сидоров Игорь Александрович**

студент,

Лысьвенского филиала ФГАОУВО Пермского национального  
исследовательского политехнического университета,  
РФ, г. Лысьва

**Лепихин Александр Васильевич**

старший преподаватель,

Лысьвенского филиала ФГАОУ ВО Пермского  
национального исследовательского политехнического университета,  
РФ, г. Лысьва

**Аннотация.** В данной статье представлены основные типы гидроэлектростанций. Принцип работы. Их достоинства и недостатки.

**Ключевое слово:** гидроэлектростанции, генерация, электричество, река, поток, движение.

Гидроэлектростанции – это энергетические гиганты, которые используют энергию потока водных масс для генерации электроэнергии и последующее её использования. Они могут быть масштабного, среднего и малого габарита, и они являются одними из наиболее эффективных и экологически чистых вариантов производства электроэнергии.

### Как работают гидроэлектростанции?

Гидроэлектростанции работают на принципе преобразования кинетической энергии водных масс в электрическую энергию. Вот основные принципы работы гидроэлектростанций:

Водную массу собирают в водохранилище, чтобы накопить потенциальную энергию. Это может быть искусственно созданное водохранилище, на реке, или естественным образом сформированный резервуар.

Затем необходимая водная масса направляется через трубопровод на лопасти гидротурбины, что приводит ее в движение и вращает генератор, который производит электроэнергию.

Далее энергия перенаправляется через высоковольтные линии потребителю.

### Основные типы гидроэлектростанций

Существуют два основных типа гидроэлектростанций:

Резервуарно-накопительные гидроэлектростанции. Эти станции используют водохранилища для аккумуляции и хранения воды, которая затем используется для генерации электроэнергии. Это наиболее популярный тип гидроэлектростанций, который обеспечивает наибольшие мощности и наименьший уровень шума во время работы турбин.

Проточные гидроэлектростанции. Эти станции получают воду непосредственно из потока реки, протоки или канала и приводят ее в движение через лопасти гидротурбины. Это наиболее экологический вариант гидроэлектростанций, поскольку практически не выдает отходов или выхлопных газов.

### Достоинства гидроэлектростанций

Гидроэлектростанции имеют множество достоинств по сравнению с другими источниками энергии:

Экологически чистый вариант. Гидроэлектростанции практически не производят вредных отходов или выхлопных газов, что делает их одними из самых экологически чистых источников энергии.

Стабильный и надежный источник энергии. Гидроэлектростанции обладают наивысшей производительностью, поскольку вода постоянно поступает с потоком, что обеспечивает стабильность и надежность в производстве электроэнергии.

Эффективный источник энергии. Гидроэлектростанции могут производить огромное количество энергии, особенно в сравнении с другими источниками, такими как солнечная или ветровая энергия.

### **Недостатки гидроэлектростанций**

Несмотря на все достоинства, у гидроэлектростанций есть свои недостатки:

Высокие затраты на строительство. Крупномасштабные гидроэлектростанции требуют больших вложений и времени на строительство, особенно если это резервуарно-накопительные гидроэлектростанции.

Изменение экосистемы. Постройка гидроэлектростанций может привести к изменению экосистемы, так как это может вызвать изменения в уровне воды, что может влиять на животный, растительный мир и жизнь людей.

Цена обслуживания. Гидроэлектростанции требуют специализированного обслуживания и ремонта, что может быть дорогим, особенно если станция находится в труднодоступном месте.

### **Заключение**

Гидроэлектростанции – это эффективный и экологически чистый источник энергии, который может обеспечить стабильное и надежное производство электроэнергии. Однако они также имеют свои ограничения и недостатки, которые необходимо учитывать при принятии решения о реализации проекта.

### **Список литературы:**

1. "Гидроэлектростанции: технологии и перспективы" Хакки С.М., Журнал "Электроэнергетика", 2015 г.
2. Бутысин А.В. Влияние гидроэлектростанций на окружающую среду // Успехи современного естествознания. – 2011. – № 7. – С. 84-85;
3. Брызгалов В.И., Гордон Л.А. Гидроэлектростанции. Учебное пособие. ИПЦ КГТУ. Красноярск. 2002г.
4. Вагнер А.А. Проблемы, связанные с развитием альтернативной энергетики в России. – М.: Апрель, 2016. – 16 с.
5. Стоцкий Кирилл Степанович. Гидроэлектростанция // Наука через призму времени.- 2018.-№12 (21).



## ТРАНЗИСТОРНЫЕ УСИЛИТЕЛИ НИЗКОЙ ЧАСТОТЫ

### **Терентьева Татьяна Михайловна**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

### **Убашиева Татьяна Дабаевна**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

### **Кондрашева Алеся Ивановна**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения  
РФ, г. Улан-Удэ

### **Павлова Светлана Валерьевна**

научный руководитель,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения  
РФ, г. Улан-Удэ

Цель исследования: изучить транзисторные усилители низкой частоты.

Задачи исследования: изучить устройство, работу и применение транзисторные усилители низкой частоты.

### **Актуальность**

Транзистор – это электронный прибор, используемый для усиления и обработки электрических сигналов. Он является полупроводниковым и способен генерировать, создавать и усиливать электрические колебания различных типов. Современные транзисторы имеют широкий диапазон частот и могут быть использованы для усиления различных типов сигналов. Некоторые типы транзисторов могут иметь нелинейные вольт-амперные характеристики, что может приводить к искажениям частоты усиленного сигнала. Усилители низкой частоты (УНЧ) используют для преобразования слабых сигналов преимущественно звукового диапазона в более мощные сигналы, приемлемые для непосредственного восприятия через электродинамические или иные излучатели звука. Заметим, что высокочастотные усилители до частот 10... 100 МГц строят по аналогичным схемам, все отличие чаще всего сводится к тому, что значения ёмкостей конденсаторов таких усилителей уменьшаются во столько раз, во сколько частота высокочастотного сигнала превосходит частоту низкочастотного. Усилители на транзисторах имеют ограниченный диапазон частот, который они могут усилить, особенно когда в выходной стадии используется мощный транзистор. Это может привести к искажениям частоты усиленного сигнала при использовании сложных схем связи. Это приводит к тому, что усилитель на транзисторах имеет ограниченный диапазон частот, который он может усилить, особенно если в выходной стадии используется мощный транзистор. Нелинейность вольт-амперных характеристик также является источником больших нелинейных искажений на выходе усилителя. При использовании сложных схем связи это может привести к искажению частоты усиленного сигнала. Однако, использование сложных схем связи может усугубить эту проблему, приводя к дополнительному искажению частоты усиленного сигнала. Поэтому при проектировании усилителей необходимо учитывать ограничения тран-

зисторов и выбирать оптимальные схемы связи для минимизации искажений. Также важно учитывать физические свойства транзистора, которые определяют низкое входное и высокое выходное сопротивление усилительной ступени. В целом, современные усилители на транзисторах обладают широким диапазоном частот и могут использоваться для усиления различных типов сигналов.

### Принцип работы

Транзисторного усилителя заключается в возможности усиления электрических сигналов путем изменения токов транзистора. Изменение напряжения эмиттерного перехода вызывает изменение токов транзистора, что используется для усиления сигналов.

Для преобразования изменений коллекторного тока в изменяющееся напряжение в коллекторную цепь транзистора включают нагрузку, которой может служить резистор или колебательный контур. Также для усиления переменных электрических сигналов между базой и эмиттером транзистора нужно включить источник постоянного напряжения, называемый источником смещения, который устанавливает режим работы транзистора.

Для питания коллекторной цепи транзистора можно использовать только один источник, что уменьшает размеры и массу устройства и упрощает его конструкцию. Одна из таких схем усилителя показана на рисунке.

Для усиления переменных электрических сигналов между базой и эмиттером транзистора необходимо включить конденсатор, который пропускает переменные сигналы, но блокирует постоянное напряжение источника смещения. Это позволяет сохранить режим работы транзистора в исходном состоянии, но усилить переменные сигналы, проходящие через базу и эмиттер.

Таким образом, транзисторный усилитель заключается в возможности изменять токи транзистора для усиления электрических сигналов. Для этого необходимо включить нагрузку в коллекторную цепь транзистора и конденсатор в базовую цепь. При этом необходимо поддерживать режим работы транзистора в исходном состоянии с помощью источника смещения.

### Конструкция

Тема: транзисторные усилители низкой частоты.

Цель: собрать и спаять схему транзисторных усилителей низкой частоты.

Транзисторы низкой частоты.

Принципиальные схемы 2х вариантов такого усилителя. Они по существу являются повторением схемы разобранного сейчас транзисторного усилителя (рис. 1). Только на них указаны данные детали и введены 3 дополнительных элемента: К1, С3, 51. Резистор К1 - нагрузка источника колебаний звуковой частоты; С3 – конденсатор, блокирующий головку В1 громкоговорителя по высшим звуковым частотам; 51-выключатель питания. В усилители работают транзисторы структуры р-п-р, и п-р-п. В связи с этим полярность включения питающих их батарей разная: на коллекторы транзисторов первого варианта усилителя подаётся отрицательное, а на коллекторы транзисторов второго варианта – положительное напряжение.

Полярность включения электролитических конденсаторов также разная.

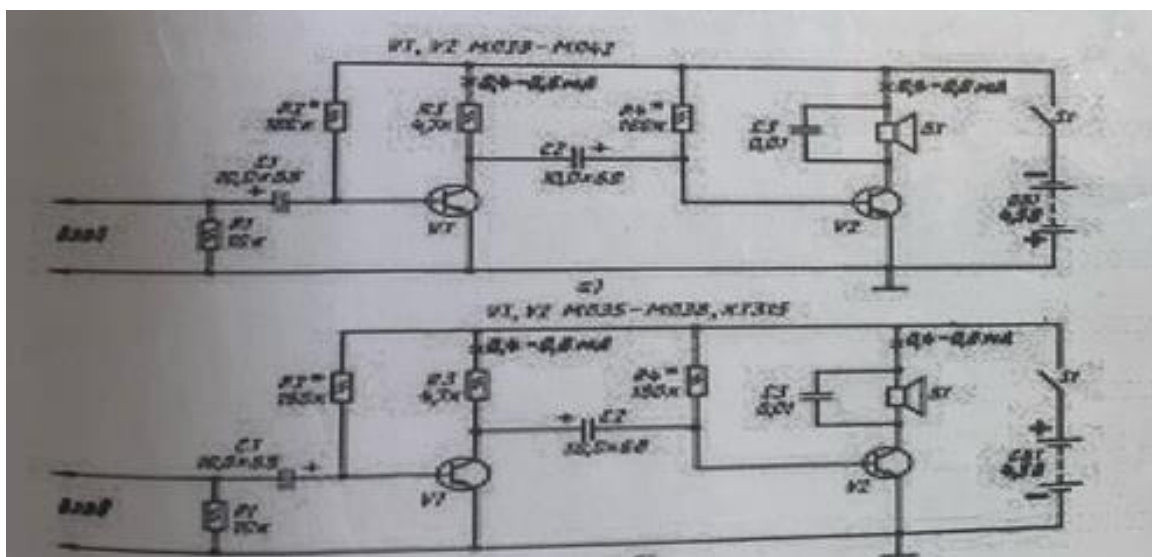


Рисунок 1. Схема

### Заключение

В данной статье был разработан усилитель низкой частоты, который соответствует всем техническим требованиям. КПД разработанного устройства превышает заданный уровень, обеспечивая его эффективную работу. Результаты исследования соответствуют нормативным документам. Усилитель низкой частоты был спроектирован с учетом частотных искажений, а применение операционной схемы позволило достичь необходимого коэффициента усиления.

### Приложение

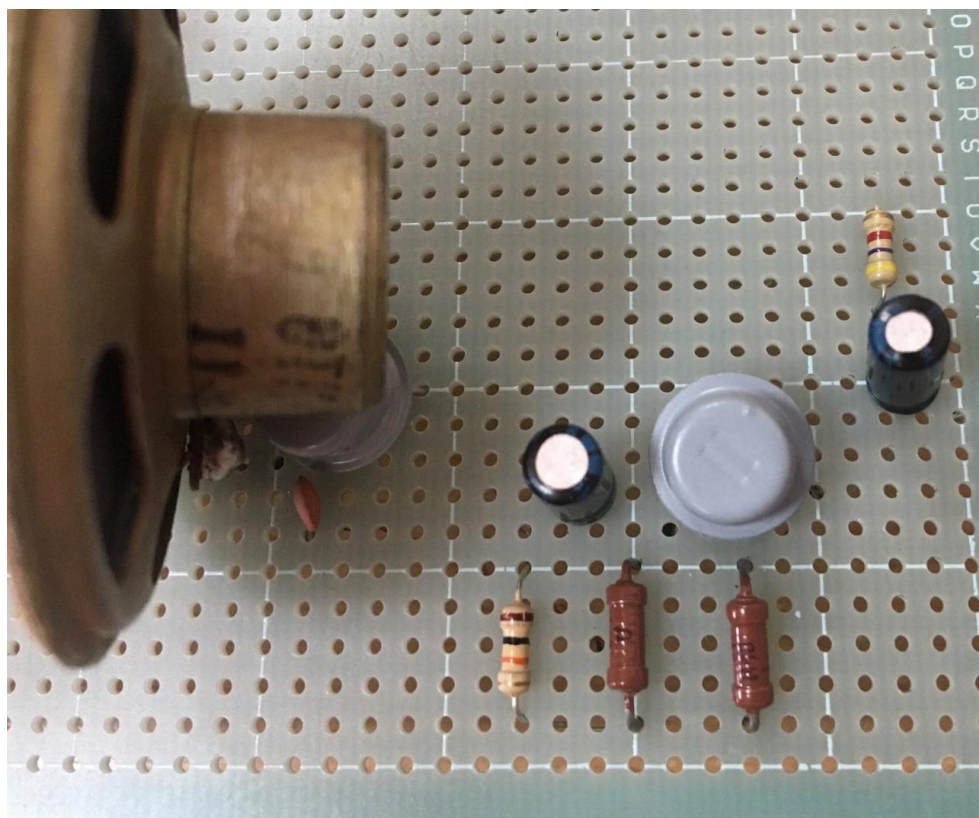


Рисунок 2. Усилитель

**Список литературы:**

1. Бабырин, А.А. Электроника и микроэлектроника Физико-технологические основы / А.А. Бабырин. - М.: Физматлит, 2008. – 424 с.
2. Бодилковский, В.Г. Электронные приборы и усилители на железнодорожном транспорте / В.Г. Бодилковский. – М. : Транспорт, 1995. – 431 с.
3. Беринов, В.И. Электронная и микропроцессорная техника на подвижном составе / В.И. Беринов. -М.:УМК МПС, 1997. -216 с

## МАРКОВСКАЯ МОДЕЛЬ НАДЕЖНОСТИ ДЛЯ СТРОГОЙ АУТЕНТИФИКАЦИИ ПО СЕРТИФИКАТУ ДОСТУПА

**Цыганок Дарья Игоревна**

студент,  
Московский государственный технический  
университет им. Н.Э. Баумана,  
РФ, г. Москва

**Бойков Илья Александрович**

студент,  
Московский государственный технический  
университет им. Н.Э. Баумана,  
РФ, г. Москва

В современном информационном обществе безопасность является одной из основных проблем. В частности, защита информации и контроль доступа к ней – одни из самых важных задач в области информационных технологий. Одним из наиболее распространенных методов контроля доступа является аутентификация, при которой пользователь проходит проверку подлинности своих учетных данных.

В данной статье будет предложена модель для оценки надежности процесса аутентификации.

Прежде чем перейти к созданию модели, следует разобраться в процессе строгой аутентификации, описать систему и её функционирование. Далее будет предложена модель надежности.

**Процедура аутентификации.** Согласно [1], аутентификация – это процесс проверки подлинности субъекта (объекта) доступа, а также принадлежности ему предъявленных идентификатора и аутентификационной информации.

Процесс аутентификации, в общем виде должен включать:

- формирование и регистрацию аутентификационной информации;
- хранение аутентификационной информации;
- предъявление идентификатора и аутентификационной информации при запросе доступа;
- проверку подлинности субъекта доступа;
- проверку принадлежности предъявленных идентификатора и аутентификационной информации;
- принятие решения.

**Процедура строгой аутентификации.** Под строгой аутентификацией, мы будем понимать аутентификацию с применением метода взаимной двухфакторной аутентификации и использованием криптографических протоколов аутентификации. При взаимной аутентификации, как субъект доступа, так и объект доступа выполняют функции доказывающей, стороны, а также проверяющей стороны. Многофакторная аутентификация требует использования как минимум двух различных факторов, и доступ к объекту разрешается только после успешной проверки обоих факторов.

Строгая аутентификация может обеспечиваться использованием сертификатов доступа. Сертификаты выдаются специальными уполномоченными организациями – центрами сертификации (Certificate Authority, CA) [3], [4]. Аутентификация на основе сертификата основывается на использовании открытых и закрытых ключей, которые связаны между собой. Сертификат содержит информацию об идентификации субъекта (например, имени и электронной почты) и открытый ключ. Он также содержит информацию о сертификационном центре, который выпустил сертификат, и о временном периоде его действия.

Аутентификация обычно осуществляется в режиме запрос-ответ. [4] Для того чтобы аутентифицироваться, пользователь, генерирует цифровую подпись случайного запроса от

сервера аутентификации с использованием своего закрытого ключа. Затем пользователь отправляет на сервер свой сертификат открытого ключа вместе с сгенерированной цифровой подписью. Сервер аутентификации проверяет подлинность сертификата открытого ключа,. Если подлинность сертификата подтверждается, то сервер проверяет подлинность цифровой подписи, используя открытый ключ пользователя, который находится в сертификате. Если цифровая подпись действительна, то аутентификация пользователя считается успешной, и сервер предоставляет субъекту доступ к защищенным ресурсам. При взаимной аутентификации клиент проверяет сертификат сервера. Доступ к криптографическим ключам осуществляется с использованием «Смарт-карты» или «USB-ключа», которые защищены паролем [1].

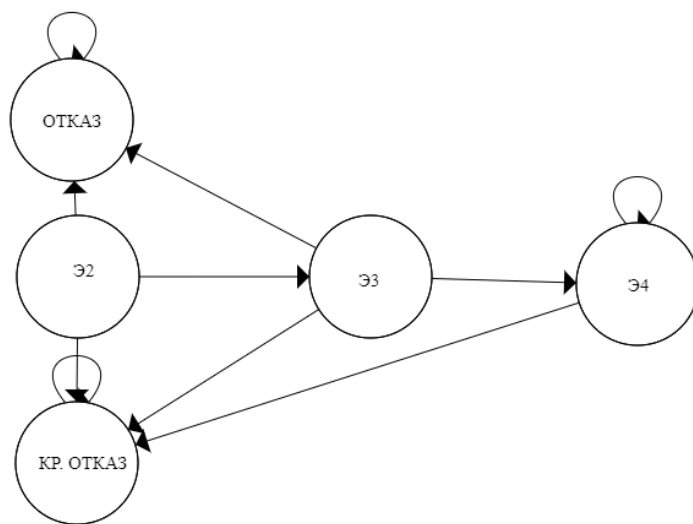
Таким образом, первый фактор аутентификации – это знание пароля от смарт-карты. Второй фактор аутентификации – это наличие смарт-карты с сертификатом доступа.

Процесс строгой аутентификации с использованием сертификатов на основе общего процесса можно разделить на следующие этапы [5] :

1. Регистрация и получение сертификата.
2. Ввод ПИН-кода для разблокировки смарт-карты (первый фактор аутентификации).
3. Установление защищенного соединения.
4. Доступ к защищенным ресурсам.

**Построение марковской модели надежности.** В данной статье предлагается рассматривать различные этапы процесса аутентификации, которые были приведены ранее, вероятности переходов между этапами будут определяться вероятностями успеха и неудачи проверки подлинности каждого этапа. После определения моделей для каждого этапа, можно будет оценить надежность системы в целом. Это позволит получить общую оценку надежности системы аутентификации и определить возможные слабые места, которые могут быть улучшены для повышения общей надежности и безопасности.

Выходными данными марковского анализа являются вероятности пребывания системы в различных состояниях, а следовательно – оценки вероятностей отказа и/или безотказной работы существенных компонентов системы.[2]



**Рисунок 1. Граф состояний строгой аутентификации по сертификатам доступа**

Составим матрицу переходных вероятностей:

$P_{ij}$  – вероятность перехода из состояния  $i$  в состояние  $j$ .

Проведем анализ с помощью метода расчета показателей надежности с помощью фундаментальной матрицы поглощающих Марковских цепей.

Матрица переходных вероятностей разбивается на 4 части:  $Q$ ,  $R$ ,  $0$  и  $I$  (рис.2), где  $Q$  – матрица вероятностей перехода между непоглощающими состояниями,  $R$  – матрица вероят-

ностей перехода из непоглощающих состояний в поглощающие,  $0$  – нулевая матрица, и  $I$  – единичная матрица. [6]

$$\begin{array}{c}
 \text{Поглощение} \\
 \text{Поглощающие} \quad \text{Не поглощающие} \\
 \text{П} = \left( \begin{array}{c|c} I & 0 \\ \hline R & Q \end{array} \right) \\
 \text{Не поглощение}
 \end{array}$$

**Рисунок 2. Матрица переходных вероятностей**

Найдем матрицу  $N$  – фундаментальная матрица поглощающей Марковской цепи

$$N = (I - Q)^{-1} \tag{1}$$

Найдем матрицу  $B$  – вероятности попадания Марковской цепи в поглощающие состояния.

$$B = NR \tag{2}$$

Таким образом, матрица  $B$  позволяет оценить вероятности перехода из каждой стадии процесса (непоглощающих состояний) в финальные поглощающие состояния.

Предложенный метод аутентификации на основе марковских моделей может быть полезными для практического применения в области безопасности информации.

При этом важно учитывать, что в реальных системах взаимодействие программного и аппаратного обеспечения может быть сложным, и оценки могут требовать дополнительных уточнений и анализа.

**Список литературы:**

1. ГОСТ Т Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения: национальный стандарт Российской Федерации: дата введения 01.05.2020/ Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва: Стандартиформ, 2020. – 32 с.
2. ГОСТ Р МЭК 31010-2021. Надежность в технике. Методы оценка риска: национальный стандарт Российской Федерации: дата введения 01.01.2022. – 94 с.
3. Андресс Джейсон. Защита данных. От авторизации до аудита. – СПб.: Питер, 2021. – 272 с.
4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова ; под редакцией А.А. Шелупанова [и др.]. – 2-е изд., стер. – Москва : Горячая линия-Телеком, 2012.
5. Горбатов В.С., Полянская О.Ю. Основы технологии РКІ. – М.: Горячая линия – Телеком, 2004. – 248 с
6. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа / И.Б. Шубинский. – М.: «Журнал Надежность», 2012, – 296 с.

## РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОГИСТИЧЕСКОЙ КОМПАНИИ СДЭК

*Шабалин Александр Дмитриевич*

*магистрант,*

*Московский институт электронной техники,*

*РФ, г. Москва*

Информационная безопасность является важным аспектом в современном мире бизнеса, особенно для логистических компаний, которые работают с конфиденциальной информацией своих клиентов и партнеров. Конфиденциальность, целостность и доступность данных являются ключевыми показателями безопасности информации, которые должны быть обеспечены в рамках бизнес-процессов любой логистической компании. Несоблюдение требований информационной безопасности может привести к серьезным последствиям, таким как утечка конфиденциальной информации, потеря доверия клиентов и партнеров, а также негативное влияние на репутацию компании [1].

Данная работа имеет большое значение для логистических компаний, так как поможет улучшить безопасность информации и снизить риски утечки, которые могут негативно сказаться на доверии клиентов и имидже компании в целом. В настоящее время информационная безопасность становится все более актуальной проблемой, ведь современные технологии позволяют киберпреступникам получить доступ к защищенной информации. Из-за этого компании теряют конфиденциальность своих данных, что приводит к финансовым потерям и ущербу для бизнеса в целом.

Важно учитывать, что проведение аудита информационной безопасности является необходимым шагом для обеспечения безопасности информационных ресурсов компании и защиты от потенциальных угроз [2].

Аудит информационной безопасности является важным инструментом, который позволяет определить уровень защищенности информации в компании. Разработка методики проведения аудита информационной безопасности в логистической компании СДЭК включает в себя несколько этапов.

### **Шаг 1. Определение целей и задач аудита**

Первым шагом при разработке методики проведения аудита информационной безопасности в логистической компании СДЭК является определение целей и задач аудита. Цели аудита могут быть различными, например, определение уровня защищенности информации, выявление уязвимых мест в информационной системе, оценка эффективности мер по защите информации и т.д.

### **Шаг 2. Определение объема и границ аудита**

На этом этапе определяется, какие именно информационные системы и данные будут аудироваться, а также устанавливаются границы аудита. В логистической компании СДЭК это могут быть системы управления складом, программы для отслеживания грузов, системы связи с клиентами и т.д.

### **Шаг 3. Оценка рисков и угроз**

Для определения наиболее уязвимых мест в информационной системе компании СДЭК необходимо провести оценку рисков и угроз. Эта оценка может включать в себя анализ угроз внешних и внутренних пользователей, оценку уязвимостей системы, оценку возможных последствий нарушения безопасности и т.д.

### **Шаг 4. Определение методов и инструментов аудита**

На этом этапе определяются методы и инструменты, которые будут использоваться при проведении аудита. Это могут быть различные программные средства для автоматизации аудита, методы тестирования на проникновение, методы анализа логов и т.д.



## Шаг 5. Разработка плана проведения аудита

На последнем этапе разрабатывается план проведения аудита, в котором определяются конкретные шаги, необходимые для проведения аудита информационной безопасности в логистической компании СДЭК. План должен включать в себя описание методов и инструментов аудита, список проверяемых систем и данных, а также описание последовательности действий при проведении аудита [3].

План проведения аудита информационной безопасности в логистической компании СДЭК должен включать в себя следующие шаги:

1. Определение целей и задач аудита.
2. Определение объема и границ аудита.
3. Оценка рисков и угроз.
4. Определение методов и инструментов аудита.
5. Подготовка программного обеспечения и оборудования для проведения аудита.
6. Проведение аудита.
7. Анализ результатов аудита и подготовка отчета.
8. Разработка рекомендаций по устранению выявленных уязвимостей и улучшению системы безопасности.
9. Контроль и внедрение рекомендаций.

В заключение можно сказать, что разработка методики проведения аудита информационной безопасности в логистической компании СДЭК является важным шагом для обеспечения безопасности информации и защиты от угроз. Применение разработанной методики позволит определить уязвимые места в системе безопасности компании и разработать меры по их устранению.

Результаты аудита показали наличие ряда уязвимостей в системе информационной безопасности компании СДЭК, связанных с недостаточной защитой и управлением доступом, отсутствием контроля за целостностью данных и защитой персональных данных, а также с наличием уязвимостей в сетевой инфраструктуре компании. Были разработаны рекомендации по устранению этих уязвимостей, а также по улучшению процедур управления информационной безопасностью в целом [4].

Общая эффективность разработанной методики проведения аудита информационной безопасности в логистической компании СДЭК может быть оценена как высокая. Она позволила выявить ряд уязвимостей в системе информационной безопасности компании и разработать рекомендации по их устранению. Более того, методика может быть использована не только в компании СДЭК, но и в других логистических компаниях, что делает ее универсальной.

Таким образом, разработанная методика проведения аудита информационной безопасности в логистической компании СДЭК позволила выявить ряд уязвимостей в системе информационной безопасности компании и разработать рекомендации по их устранению. Дальнейшее развитие методики может быть направлено на расширение ее функционала, улучшение инструментальных средств и повышение квалификации персонала.

### Список литературы:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2018. – 400 с.
2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – М.: ГЛТ, 2018. – 586 с.
3. Ерохин, В.В. Безопасность информационных систем. Учебное пособие / В.В. Ерохин, Д.А. Погоньшева, И.Г. Степченко. – М.: Флинта, Наука, 2018. – 184 с.
4. Малюк, А.А. Введение в информационную безопасность. Учебное пособие для вузов. Гриф УМО МО РФ / А.А. Малюк. – М.: Горячая линия – Телеком, 2021. – 853 с.

## СОЗДАНИЕ МАКЕТА КОМПЛЕКСА ДЛЯ АВТОМАТИЗАЦИИ ИЗМЕРЕНИЙ ТРАССОВОГО ЗАТУХАНИЯ ПРИ КОНТРОЛЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

**Шишмаков Роман Олегович**

*магистрант,*

*Московский институт электронной техники,*

*РФ, г. Москва*

Ввиду накопившегося опыта измерений трассового затухания классическим методом, когда двое измерителей, находящиеся далеко друг от друга, с помощью переговоров по радиации идут по заданному диапазону частот с определённым шагом и устанавливают на генераторе и анализаторе одинаковые частоты и фиксируют значение сигнала на них, возник вопрос о возможности автоматизации измерений трассового затухания.

Задача была в том, чтобы связать между собой генератор и анализатор спектра. На первом этапе решения данной задачи было предложено заставить «общаться» генератор и анализатор между собой через ноутбук по локальной сети (LAN).

В 1990 году был представлен оригинальный стандарт SCPI (Standard Commands for Programmable Instruments), который включает набор команд для программируемых инструментов. SCPI команды представлены в виде ASCII-строк и передаются в устройство через физический уровень связи [1].

VISA архитектура предоставляет механизм общения с прибором в формате "запрос-ответ". Компьютер (ноутбук) отправляет специфичные команды-запросы, соответствующие определённому прибору (например, запрос на выполнение измерения амплитуды сигнала), и ожидает ответа от прибора, который может содержать отчет о состоянии или результаты измерений. Практически все современные измерительные приборы поддерживают архитектуру VISA, при кодировании к ним компьютера (ноутбука), например, по интерфейсу LAN. Достаточно лишь установить драйвер на ноутбук, подключить генератор сигналов, анализатор спектра и ноутбук к одной локальной сети и написать программу для совместной работы по VISA-архитектуре измерительных устройств и проведения измерений.

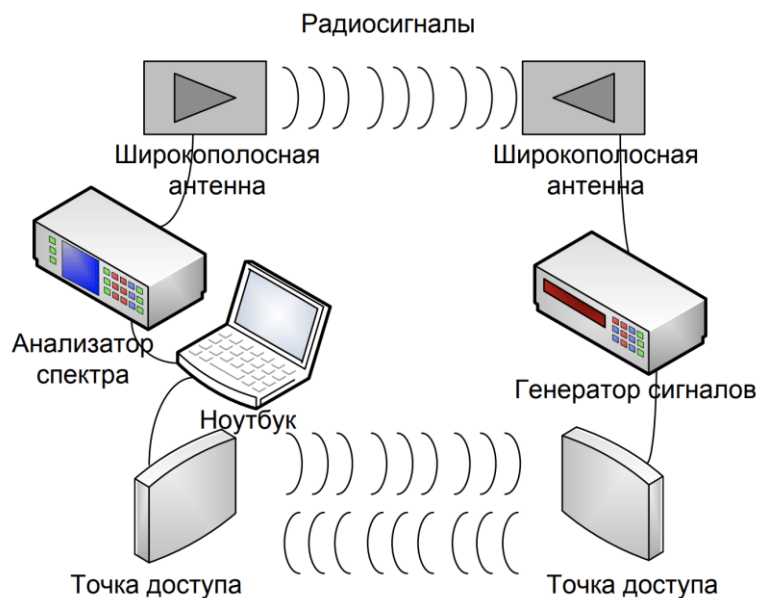
Итого, следует, что к имеющемуся измерительному и вспомогательному оборудованию добавляется ноутбук (с программой, написанной в Microsoft Visual Studio 2017, язык программирования C#), к которому подключены передающая сторона (генератор) и принимающая (анализатор) по LAN.

Кажется, что решение довольно простое, но есть проблема, которая была ясна изначально – все подключения проводные.

Даже в случае небольшой контролируемой зоны (например, ограждающих конструкций помещения) нужен кабель большой длины, такой, чтобы можно было проводить измерения не только в соседних помещениях на том же этаже, на котором располагается СВТ, но и на других этажах. В случаях, когда контролируемой зоной является большая территория, всё обстоит намного хуже. Это неудобно. Генератор сигнала и анализатор спектра должны синхронизироваться по частоте без проводов.

Таким образом, появилась новая версия макета комплекса для измерений трассового затухания.

Схема макета комплекса автоматизированных измерений трассового затухания при контроле защищённости информации, обрабатываемой СВТ, от утечки за счёт ПЭМИН (на примере измерений сигнала в пространстве) (рис. 1) [2].



**Рисунок 1. Макет комплекса для измерений трассового затухания (в пространстве)**

Передающая сторона комплекса показана на правой части схемы, приёмная, соответственно – слева. Схема комплекса для измерений трассового затухания в линиях будет аналогичной, только вместо антенн будут использоваться индуктор и токосъёмник (пробник напряжения).

Измерительный комплекс состоит из измерительного и вспомогательного оборудования, ноутбука с доработанной программой и двух беспроводных точек доступа.

Ноутбук и анализатор спектра, как и в прошлой версии комплекса, находятся в одной локальной сети и подключаются по LAN-порту, управление анализатором с ноутбука осуществляется через протокол VISA. Ноутбук и генератор сигналов имеют связь по беспроводному последовательному порту через точки доступа. Точки доступа подключается к генератору и анализатору по интерфейсу USB.

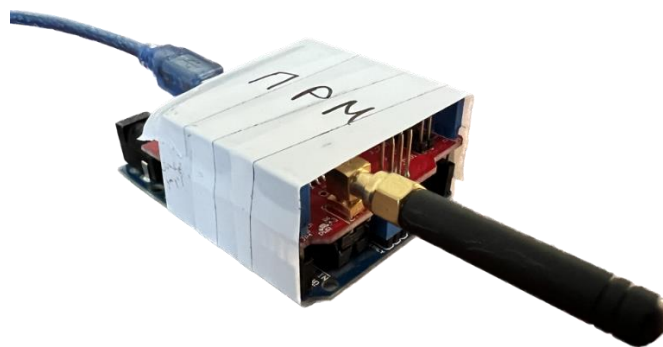
Следует подробнее описать точки доступа. Каждая из них состоит из двух микроконтроллеров Arduino, осуществляющих передачу (приём) информации по интерфейсу USB и по радиоканалу на частоте 433 МГц, в соответствии со вшитой в них программой, написанной на языке программирования Arduino C.

Точка доступа, подключаемая к генератору сигналов, приведена на рисунке 2 (рис. 2).



**Рисунок 2. Точка доступа, подключаемая к генератору сигналов**

Точка доступа, подключаемая к анализатору спектра, приведена на рисунке 3 (рис. 3).



**Рисунок 3. Точка доступа, подключаемая к анализатору спектра**

Технологический процесс работы составных частей макета измерительного комплекса заключается в следующем алгоритме:

- команды управления генератором поступают от ноутбука на генератор сигналов по последовательному беспроводному порту, состоящему из радиоканала и двух интерфейсов USB;
- одновременно команды управления анализатором поступают от ноутбука на анализатор спектра напрямую по LAN-порту, затем, информационные потоки, содержащие в себе результаты измерений, возвращаются от анализатора в ноутбук.

Стоит отметить, что, в случае необходимости, макет комплекса для измерений трассового затухания может работать и по проводной схеме, достаточно лишь ноутбук и генератор подключить по LAN-порту.

#### **Список литературы:**

1. Киргизбаев В.П. Применение команд SCPI для автоматизации проведения лабораторных специальных исследований с использованием анализаторов спектра. – Иркутск: ИГУПС. – 2022. – 11 С.
2. Марков В.П., Данеев А.В. Автоматизированный комплекс для определения величины затухания сигнала // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №2(7). – С. 46-55.

## РУБРИКА

## «ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ»

## НЕСИММЕТРИЧНЫЙ МУЛЬТИВИБРАТОР-МЕТРОНОМ

**Виноградов Александр Юрьевич**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Белобородов Денис Павлович**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Павлова Светлана Валерьевна**

научный руководитель,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Аннотация.** Несимметричный мультивибратор-метроном является электронной схемой, которая используется для создания периодического сигнала с несимметричной формой импульса. Он может использоваться в качестве метронома для музыкальных инструментов или для других приложений, где требуется точный и стабильный сигнал с заданной частотой и длительностью импульса. С помощью этой схемы можно также регулировать частоту и длительность импульса, что делает ее универсальным инструментом для различных задач.

**Ключевые слова:** Несимметричный мультивибратор, метроном, ритмический эффект, форма волны, генерация импульсов, частота, амплитуда, длительность, музыкальное оборудование.

**Цель исследования:** Изучение принципа работы устройства и его характеристик, а также рассмотрение возможных областей применения в музыкальном оборудовании и индустрии.

**Задачи исследования:** Изучение принципа работы несимметричного мультивибратора-метронома. Рассмотрение основных характеристик устройства: частоты генерации импульсов, амплитуды и длительности импульсов.

### **Обзор Несимметричного мультивибратора и их применения в электронике**

Несимметричный мультивибратор (асимметричный мультивибратор) – это электронная схема, которая генерирует периодические импульсы с различной длительностью фронтов. Такой тип мультивибратора состоит из двух усилительных каскадов, каждый из которых содержит один транзистор. Различие в длительности фронтов формируется благодаря различию значений емкостей и/или резисторов в цепях управления.

Метроном – это электронное устройство, используемое для удержания стабильного ритма при производстве музыкального исполнения. Он генерирует метрономический ритм,

который играет роль определителя темпа музыки. Мультивибраторы могут использоваться для создания метрономического сигнала в электронных метрономах.

В электронике несимметричные мультивибраторы-метрономы могут использоваться для создания сигналов таймеров, звуковых генераторов, а также для решения других задач управления и контроля времени в системах автоматизации и управления. Мультивибраторы также могут быть использованы в качестве ключевых компонентов в различных видео- и звуковых системах, таких как генераторы частоты, модуляторы сигналов, детекторы сигналов и другие устройства.

Таким образом, несимметричные мультивибраторы-метрономы являются важными элементами в электронике, благодаря своей способности генерировать стабильные импульсы различной формы и длительности, что позволяет решать различные задачи управления временем в системах автоматизации и управления.

### Описание компонентов

1. Два транзистора: один используется в качестве ключа, а другой – как усилитель.
2. Два конденсатора: один из них используется для формирования обратной связи, а второй – для изменения частоты колебаний.
3. Два резистора: один из них используется для определения времени зарядки и разрядки конденсаторов, а второй – для ограничения тока.
4. Динамик: используется для преобразования электрического сигнала в звуковой. Эти элементы в совокупности образуют несимметричный мультивибратор-метроном, который может быть использован в различных электронных устройствах.

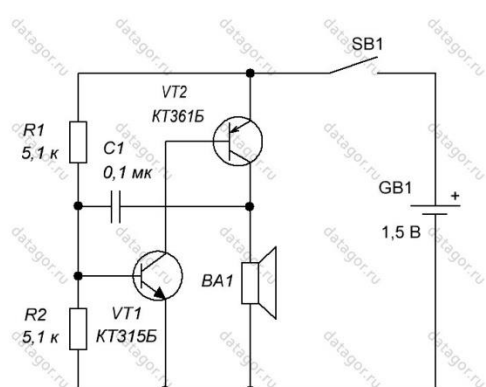


Рисунок 1. Схема

### Принцип работы метронома на основе несимметричного мультивибратора

Метроном на основе несимметричного мультивибратора генерирует ритмически повторяющиеся звуковые сигналы, помогая музыкантам при игре в музыкальных произведениях. Он использует несимметричный мультивибратор – колебательную систему, которая через открытие и закрытие ключа с определенной периодичностью изменяет емкость конденсатора и частоту колебаний. Изменение параметров этой системы позволяет менять скорость и ритм сигналов, что делает метроном универсальным инструментом для музыкантов разных уровней и стилей.

### Как использовать несимметричный мультивибратор-метроном для измерения времени и частоты

Для измерения времени с помощью несимметричного мультивибратора-метронома необходимо включить его, выбрать режим работы мультивибратора и установить нужную частоту импульсов. Затем, при каждом импульсе, который будет звучать через динамик,

можно отмечать прошедшее время с помощью секундомера или другого устройства для измерения времени.

Для измерения частоты необходимо также включить метроном, выбрать режим работы и установить нужную частоту импульсов. Затем можно использовать осциллограф или другое устройство для измерения частоты и анализа формы сигнала. Также можно использовать специальные программы на компьютере для измерения частоты звуковых сигналов.

### **Рассмотрение возможных областей применения в музыкальном оборудовании и индустрии**

Несимметричный мультивибратор-метроном широко используется в музыкальных инструментах и оборудовании для создания ритмических паттернов. Например, он может использоваться в электронных барабанах для генерации ударных звуков или в синтезаторах для создания различных ритмических эффектов.

Он также может использоваться в качестве источника тайминга для синхронизации различных компонентов музыкального оборудования, что помогает достичь более точной и стабильной работы системы.

В индустрии звукозаписи несимметричный мультивибратор-метроном может использоваться в качестве инструмента для измерения частоты и времени длительности звуковых сигналов. Эти данные могут быть использованы для установления темпа, скорости и точности записываемой музыки.

Также несимметричный мультивибратор-метроном может быть полезен в качестве инструмента для создания аудиовизуальных эффектов в кино и телевидении. Он может использоваться для создания различных эффектов, таких как эффект пульсации, мерцания или вспышек.

В целом, несимметричный мультивибратор-метроном имеет широкий спектр применения в музыкальной индустрии и оборудовании, а также в других областях, где требуются точные измерения времени и частоты.

### **Рассмотрение основных характеристик устройства**

Частота генерации импульсов может быть настроена в широком диапазоне, обычно от нескольких герц до нескольких килогерц. Это позволяет использовать несимметричный мультивибратор-метроном для создания различных ритмических сигналов и метрономов.

Амплитуда импульсов также может быть настроена в определенных пределах. Обычно она находится в диапазоне от нескольких микровольт до нескольких вольт. Высокая амплитуда может привести к искажению сигнала или повреждению приемника, поэтому необходимо тщательно контролировать этот параметр. Длительность импульсов также является важной характеристикой несимметричного мультивибратора-метронома. Она может быть настроена в широком диапазоне, от нескольких микросекунд до нескольких сотен миллисекунд. Длительность импульсов определяет периодичность и ритмичность генерируемого сигнала. В заключение можно отметить, что несимметричный мультивибратор-метроном является универсальным электронным устройством, которое может использоваться для создания различных ритмических сигналов и метрономов. Его характеристики зависят от конструкции и используемых элементов, поэтому при проектировании необходимо тщательно подобрать параметры для достижения желаемых результатов. В целом, несимметричный мультивибратор-метроном является полезным инструментом для музыкантов, звукорежиссеров и других специалистов в области звукового оформления.

### **Список литературы:**

1. Бессонов В. «Кружок радиоэлектроники». – М.: Просвещение, 1993.
2. Под ред. Шилейко А.В. Электронные устройства железнодорожной автоматики, телемеханики и связи. – М.: Транспорт, 1989.
3. Чистяков Н.И. «Справочник радиоконструктора», Радио и связь, выпуск 1043.

## СВЕТОДИОДЫ В СВЕТОВОЙ СИГНАЛИЗАЦИИ

**Хомогоров Артур Максимович**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Агунов Алексей Александрович**

студент,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Павлова Светлана Валерьевна**

научный руководитель,

Улан-Удэнский колледж железнодорожного транспорта  
Иркутского государственного университета путей сообщения,  
РФ, г. Улан-Удэ

**Аннотация.** Статья посвящена использованию светодиодов в световой сигнализации. В статье описываются принципы работы светодиодов, их преимущества по сравнению с другими источниками света, а также возможности их применения в различных видах световой сигнализации. Рассказывается об их использовании в автомобильных фарах и задних фонарях, световых указателях и сигналах тревоги, а также в других областях, где требуется световая сигнализация. Описывается, как светодиоды обеспечивают яркость, надежность, длительный срок службы и экономичность, и как их использование может снизить энергозатраты и повысить безопасность на дорогах, в зданиях и других местах. В статье также даются рекомендации по выбору светодиодной световой сигнализации и ее установке, чтобы обеспечить максимальную эффективность и надежность ее работы.

**Ключевые слова:** светодиоды, светодиодная лампа, световая сигнализация, аварийный маяк, световой сигнал, мигание, дальность, яркость, энергопотребление, сравнение с лампами, долговечность, экологичность, надежность, конструкция, установка, виды светодиодных сигналов.

**Цель исследования:** изучение применения светодиодов в световой сигнализации с целью рассмотрения их преимуществ перед традиционными светильниками, такими как лампы, основанные на технологии газоразрядных ламп, а также изучения характеристик и особенностей установки и использования светодиодов в качестве аварийного маяка, фонаря и других световых сигналов. В результате исследования можно определить эффективность и экономическую целесообразность использования светодиодной технологии в световой сигнализации, а также предложить рекомендации по оптимальному выбору и использованию светодиодных светильников в зависимости от конкретных условий и требований к световой сигнализации.

**Задачи исследования:**

1. Проанализировать преимущества и недостатки светодиодных светильников по сравнению с традиционными светильниками в световой сигнализации.
2. Изучить особенности конструкции и установки светодиодных светильников, а также требования к их эксплуатации и обслуживанию.
3. Рассмотреть использование светодиодных светильников в качестве аварийных маяков, фонарей и других световых сигналов и оценить их эффективность в различных условиях эксплуатации.



4. Исследовать технические характеристики светодиодных светильников, такие как дальность, яркость, энергопотребление и долговечность, и сравнить их с аналогами на основе традиционных светильников.

5. Проанализировать экономическую целесообразность применения светодиодной технологии в световой сигнализации и рассмотреть возможные способы оптимизации затрат на светодиодные светильники.

6. Предложить рекомендации по выбору и использованию светодиодных светильников в зависимости от конкретных условий и требований к световой сигнализации.

### **Общие принципы работы: Краткое описание Светодиодов в световой сигнализации**

Светодиоды используются в световой сигнализации благодаря своей высокой яркости, эффективности и низкому потреблению энергии. Они работают на основе эффекта электролюминесценции, при котором электрический ток проходит через полупроводниковый материал и вызывает излучение света.

В световой сигнализации светодиоды могут быть использованы для создания различных типов световых сигналов, включая мигающие, непрерывные и ультрафиолетовые. У светодиодов более ограниченный угол излучения, что позволяет более точно направлять свет в нужном направлении.

Светодиоды также имеют довольно длительный срок службы, что позволяет снизить затраты на их замену и обслуживание. Они могут использоваться в аварийных маяках, фонарях, прожекторах и других устройствах световой сигнализации для оповещения о ЧП, обозначения местоположения, маркировки дорожных знаков и других целей.

Таким образом, основные принципы работы светодиодов в световой сигнализации сводятся к использованию эффекта электролюминесценции для создания ярких световых сигналов с высокой эффективностью и длительным сроком службы.

### **Области применения Светодиода в световой сигнализации**

Светодиоды широко применяются в световой сигнализации благодаря своим преимуществам перед традиционными источниками света. Они могут использоваться в следующих областях:

1. Автомобильная промышленность: светодиоды широко используются для создания фар, стоп-сигналов, поворотников и других световых сигналов на автомобилях. Они обладают более высокой яркостью и эффективностью, а также имеют более длительный срок службы по сравнению с традиционными источниками света.

2. Общественный транспорт: Светодиоды используются в световой сигнализации автобусов, трамваев и метро для отображения номеров маршрута, стоп-сигналов, и информационных световых табло на остановках.

3. Аэропорты: Светодиодные маяки используются в аэропортах для сигнализации о неблагоприятных метеорологических условиях, оповещения о блокировке взлетной полосы или для благоприятного направления самолетов.

4. Морские и речные суда: Светодиоды применяются для маркировки местности, как аварийное освещение, а также для оповещения о непогоде и световых сигналах.

5. и аварийно-спасательные службы: Светодиоды используются в аварийных маяках, фонарях и фонарях глубоководных обслуживающих судов, а также в качестве осветительного оборудования для работы в неосвещенных местах.

Таким образом, светодиоды широко применяются в различных областях световой сигнализации, благодаря своим преимуществам, таким как высокая яркость, низкое энергопотребление и длительный срок службы.

### **Описание принципа работы светодиода в световой сигнализации**

Светодиоды обладают высокой эффективностью, что означает, что они преобразуют большую часть электрической энергии в световую энергию. Они также имеют более низкое

энергопотребление по сравнению с традиционными источниками света, поскольку они используют меньше энергии для создания света.

Кроме того, светодиоды имеют более длительный срок службы, что позволяет снизить затраты на обслуживание и замену осветительных устройств. Они также обладают более высокой яркостью и способностью быстро мигать, что делает их идеальным выбором для использования в световой сигнализации.

Таким образом, светодиоды в световой сигнализации работают на основе эффекта электролюминесценции в полупроводниковом материале, что позволяет им создавать яркие и долговечные световые сигналы с высокой эффективностью и низким энергопотреблением.

**Заключение.** Таким образом, светодиоды являются эффективным и экономически выгодным решением для использования в световой сигнализации, благодаря их преимуществам в сравнении с традиционными источниками света.

### **Список литературы:**

1. Борисенко Д.Л., Черкин И.В., Богданов Ф.Г. Применение светодиодов в световой сигнализации // Инновационные технологии и науки. 2018. Т. 4 (2). С. 53-58.
2. Смирнов С.В., Топилин О.Н., Шуршалов В.В. Применение светодиодов в системах световой сигнализации // Наука и молодежь. 2013. Т. 26 (7). С. 176-179.
3. Ашрафова Н.Б., Шевцова Н.М. Применение светодиодов в световых индикаторах // Технологии безопасности. 2016. № 1 (19). С. 70-72.

*ДЛЯ ЗАМЕТОК*

*ДЛЯ ЗАМЕТОК*

*Электронный научный журнал*

**СТУДЕНЧЕСКИЙ ФОРУМ**

№ 22 (245)  
Июнь 2023 г.

Часть 2

В авторской редакции

Свидетельство о регистрации СМИ: ЭЛ № ФС 77 – 66232 от 01.07.2016

Издательство «МЦНО»  
123098, г. Москва, ул. Маршала Василевского, дом 5, корпус 1, к. 74

E-mail: [studjournal@nauchforum.ru](mailto:studjournal@nauchforum.ru)

16+

